UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II

Università degli studi di Napoli Federico II

Ph.D. Thesis

in

Information Technology and Electrical Engineering

Cooperative control of autonomous connected vehicles from a Networked Control perspective: Theory and experimental validation

---

Alberto Petrillo

Tutor

Prof. Stefania Santini

Coordinator

Prof. Daniele Riccio

XXXI Ciclo

Department of Information Technology and Electrical Engineering (DIETI)

"Whenever you want turn on a dream and let it burn you"

William Shakespeare

Abstract

Formation control of autonomous connected vehicles is one of the typical problems addressed in the general context of networked control systems. By leveraging this paradigm, a platoon composed by multiple connected and automated vehicles is represented as one-dimensional network of dynamical agents, in which each agent only uses its neighboring information to locally control its motion, while it aims to achieve certain global coordination with all other agents. Within this theoretical framework, control algorithms are traditionally designed based on an implicit assumption of unlimited bandwidth and perfect communication environments. However, in practice, wireless communication networks, enabling the cooperative driving applications, introduce unavoidable communication impairments such as transmission delay and packet losses that strongly affect the performances of cooperative driving. Moreover, in addition to this problem, wireless communication networks can suffer different security threats. The challenge in the control field is hence to design cooperative control algorithms that are robust to communication impairments and resilient to cyber attacks. The work aim is to tackle and solve these challenges by proposing different properly designed control strategies. They are validated both in analytical, numerical and experimental ways. Obtained results confirm the effectiveness of the strategies in coping with communication impairments and security vulnerabilities.

Contents

1 Introduction **19**
1.1 Motivation and Contributions 19
1.2 Thesis Outline 24

2 Mathematical preliminaries and Background **27**
2.1 Cooperative Control of networked dynamical systems . . . 27
2.1.1 Networked Dynamical systems Modeling 28
2.1.1.1 Digraph Propriety 30
2.1.2 Consensus and Synchronization in networked dynamical systems 31
2.2 Stability of Continuos-Time Systems 32
2.3 Time-Delay Systems Theory 34
2.3.1 Krasovskii theorem 35
2.3.2 Model transformation - Leibniz-Newton formula . 36
2.4 Integral inequalities 37

3 Cooperative Driving of Autonomous Connected Vehicles as Networked Control Systems **39**
3.1 Cooperative Driving Systems 39
3.2 Modeling of Connected Autonomous Vehicles 44
3.2.1 Agent Dynamics 45
3.2.2 Communication Topology 48
3.2.3 Formation Geometry 50
3.2.4 Distributed Controller 51
3.3 Communication issues of cooperative driving application . 52
3.4 Security issues of cooperative driving application 54

4 Adaptive synchronization-based control protocol for cooperative driving of autonomous vehicles with multiple communication delays 57
4.1 Cooperative Driving as Synchronization problem 58
4.2 Cooperative Leader Tracking 62
4.2.1 Closed-Loop Vehicular Network 64
4.3 Stability Analysis 67
4.4 Numerical Analysis 74
4.4.1 Network and Traffic Scenario 74
4.4.2 Tracking performance for L-P-F topology 78
4.4.3 Alternative communication topologies 83
4.4.4 Hard Braking maneuver for different communication topologies 84
4.4.5 Robustness with respect to lossy channels 85
4.4.6 A Brief Comparison with an up-to-date distributed control 88
4.5 Concluding Remarks 89

5 On the Robustness of the distributed Adaptive Synchronization Protocol for Connected Autonomous Vehicles with Multiple Disturbances 91
5.1 Robustness Issues in Cooperative Driving Systems 92
5.2 Cooperative driving in uncertain driving conditions 93
5.3 Robust Stability 94
5.3.1 Closed-Loop Dynamics 94
5.3.2 Proof of Robust Stability 96
5.4 Numerical Validation 99
5.5 Concluding Remarks 102

6 Distributed Resilient Control strategy for autonomous connected vehicles platoons in presence of security vulnerabilities 103
6.1 Security Issues in Cooperative Driving Systems 104
6.2 Cyber Attacks in Vehicular Network 106
6.2.1 Malicious Attacks to Vehicular Networks 106
6.2.2 Malicious Attack Countermeasures in Platooning Applications 110

6.3 Collaborative Strategy for Platooning and Countermeasure for Malicious Behaviors . . . 113
6.4 Stability Analysis . . . 117
6.4.1 Vehicular Network Dynamics . . . 117
6.4.2 Proof of Convergence . . . 118
6.5 Numerical Analysis . . . 123
6.5.1 Network and Traffic Scenario . . . 123
6.5.2 Description of the Attacks . . . 125
6.5.2.1 Spoofing . . . 125
6.5.2.2 Message Falsification . . . 125
6.5.2.3 Denial of Service . . . 126
6.5.2.4 Burst Transmission . . . 126
6.5.3 Simulation Results . . . 127
6.5.3.1 Platoon Condition without Attacks . . . 127
6.5.3.2 Platoon Condition with Attacks . . . 128
6.5.3.3 Leader Velocity Tracking Performance . . 138
6.5.3.4 A Discussion with Respect to Literature . 138
6.6 Concluding Remarks . . . 140

7 Cooperative Driving at Traffic Junction 141
7.1 Cooperative crossing of autonomous vehicles as virtual platoon problem . . . 141
7.2 System Modeling and Problem Formulation . . . 144
7.2.1 Problem Formulation as a Virtual Platoon . . . 146
7.2.2 Procedure details . . . 147
7.3 Distributed Finite Time Control Protocol for Self-driving Vehicles at Intersection . . . 148
7.4 Numerical Validation . . . 149
7.5 Concluding remarks . . . 151

8 Experimental validation of Cooperative Driving Strategies 153
8.1 Experimental setup . . . 153
8.1.1 Volvo Car XC90 . . . 154
8.1.2 Volvo Truck FH16 . . . 156
8.1.3 Volvo Car S90 . . . 158
8.2 Experimental Driving Scenario . . . 161
8.3 Experimental Results . . . 164

8.3.1 Three autonomous vehicles scenario 166
8.3.2 Two autonomous vehicles with one human-driven vehicle scenario 167
8.4 Concluding remarks 168

9 Conclusions **169**
9.1 Future Works 170

Bibliography **172**

List of Figures

2.1 Example of networked dynamical systems in engineering. 28

3.1 ITS scenario: Vehicles communicate information each other. 40
3.2 Cooperative driving systems. 42
3.3 The architecture for the cooperative driving of automated vehicles. 43
3.4 Schematic representation of autonomous connected vehicles platoons from networked control systems perspective[197]. 45
3.5 Examplar platoon communication topologies: (a) Predecessor-Following (P-F), (b): Leader-Predecessor-Following (L-P-F); (c): Bidirectional-Leader-Predecessor (B-L-F); (d): All-to-All (Broadcast, BR); (e): Platoon of $N + 1$ vehicles. 50

4.1 Keyframe of the simulation scenario. The vehicles platoon moves on a reserved lane (the right-most lane). Initial conditions are reported in Table 4.2. 75
4.2 Leader maneuvers: (a) Trapezoidal speed profile; (b) Realistic driving profile. 76
4.3 Platoon creation under L-P-F topology. Time history of the relative errors ($i = 1, \dots 7$): (a) Time history of the position error computed as $r_i(t) - r_0(t) - d_{i0}$; (b) Time history of the speed error computed as $v_i(t) - v_0$; (c) Time history of the acceleration error computed as $a_i(t) - a_0(t)$. 79

4.4 Platoon creation under L-P-F topology. Analysis of the warning index CI_i ($\forall i = 1, \cdots, 7$). 79
4.5 Platoon creation under L-P-F topology. Adaptive gains convergence ($i = 1, \ldots, 7$; $j = 0, \ldots, 7$): (a) Time history of the adaptive gains $\rho_{ij}(t)$; (b) Time history of the adaptive gains $\beta_{ij}(t)$; (c) Time history of the adaptive gains $\gamma_{ij}(t)$. 80
4.6 Tracking performance for the trapezoidal speed profile in Fig. 4.2a under L-P-F topology: (a) Time history of the vehicles speed $v_i(t)$ ($i = 0, \ldots 7$); (b) Time history of the vehicles acceleration $a_i(t)$ ($i = 0, \ldots 7$). 80
4.7 Tracking performance for the trapezoidal speed profile in Fig. 4.2a under L-P-F topology. Time histories of the relative errors ($i = 1, \ldots 7$): (a) Position error computed as $r_i(t) - r_0(t) - d_{i0}$; (b) Speed error computed as $v_i(t) - v_0(t)$; (c) Acceleration error computed as $a_i(t) - a_0(t)$. 81
4.8 Tracking performance for the trapezoidal speed profile in Fig. 4.2a under L-P-F topology. Adaptive gains convergence ($i = 1, \ldots, 7$; $j = 0, \ldots, 7$): (a) Time history of the adaptive gains $\rho_{ij}(t)$; (b) Time history of the adaptive gains $\beta_{ij}(t)$; (c) Time history of the adaptive gains $\gamma_{ij}(t)$. 82
4.9 Tracking performance for the realistic driving profile in Fig. 4.2b under L-P-F topology. Time history of the relative errors ($i = 1, \ldots, 7$): (a) Time history of the position error computed as $r_i(t) - r_0(t) - d_{i0}$; (b) Time history of the speed error computed as $v_i(t) - v_0(t)$; (c) Time history of the acceleration error computed as $a_i(t) - a_0(t)$. 83
4.10 Alternative topologies. Tracking performance for the trapezoidal speed profile in Fig. 4.2a. Time history of vehicles speed, $v_i(t)$ ($i = 0, \ldots 7$): (a) B-L-F; (b) BR; (c) P-F. 84
4.11 Alternative topologies. Tracking performance for the realistic driving profile in Fig. 4.2b. Time history of vehicles speed, $v_i(t)$ ($i = 0, \ldots 7$): (a) B-L-F; (b) BR; (c) P-F. . . 85

4.12 Tracking performance for a hard braking maneuver. Time history of vehicles speed, $v_i(t)$ $(i = 0, \dots 7)$: (a) L-P-F; (b) B-L-F; (c) BR; (d) P-F. 86
4.13 Hard braking maneuver under L-P-F topology. Analysis of the warning index CI_i $(\forall i = 1, \cdots, 7)$. 86
4.14 Bernoulli transmission channel. Tracking performance for the realistic driving profile in Fig. 4.2b under L-P-F topology: (a) Time history of the position error computed as $r_i(t) - r_0(t) - d_{i0}$ $(i = 1, \dots 7)$; (b) Time history of the speed $v_i(t)$ $(i = 1, \dots 7)$; (c) Time history of the acceleration $a_i(t)$ $(i = 1, \dots 7)$. 87
4.15 Gilbert-Elliott transmission channel. Tracking performance for the realistic driving profile in Fig. 4.2b under L-P-F topology: (a) Time history of the position error computed as $r_i(t) - r_0(t) - d_{i0}$ $(i = 1, \dots 7)$; (b) Time history of the speed $v_i(t)$ $(i = 1, \dots 7)$; (c) Time history of the acceleration $a_i(t)$ $(i = 1, \dots 7)$. 88
4.16 Consensus-based controller tracking performance for the realistic driving profile in Fig. 4.2b under L-P-F topology. Time history of the relative errors $(i = 1, \dots 7)$: (a): time history of the position error computed as $r_i(t) - r_0(t) - d_{i0}$; (b): time history of the speed error computed as $v_i(t) - v_0(t)$. 89

5.1 $\Phi(t) \in \mathbb{R}^{\upsilon \times \upsilon}$ 98
5.2 Leader tracking driving maneuver: a) time history of the vehicle velocity $v_i(t)$ $(i = 0, 1, 2, 3, 4, 5)$; b) time history of the vehicle acceleration $a_i(t)$ $(i = 0, 1, 2, 3, 4, 5)$. 100
5.3 Leader tracking driving maneuver: a) time history of the position error $\bar{r}_i(t)$, computed as $r_i(t) - r_0(t) - d_{i0}$ $(i = 1, 2, 3, 4, 5)$; b) time history of the velocity error $\bar{v}_i(t)$, computed as $v_i(t) - v_0(t)$ $(i = 1, 2, 3, 4, 5)$; c) time history of the acceleration error $\bar{a}_i(t)$, computed as $a_i(t) - a_0(t)$ $(i = 1, 2, 3, 4, 5)$; d) time history of the adaptive gains $\kappa_{ij}(t)$. 101

6.1 Maintaining tight formation maneuver under L-P-F topology: (a): time history of the position error computed as $r_i(t) - r_0(t) - d_{i0}$ ($\forall i = 1, \cdots, 7$); (b): time history of the speed error computed as $v_i(t) - v_0$ ($\forall i = 1, \cdots, 7$); (c): time history of the control effort $a_i(t)$ ($\forall i = 0, \cdots, 7$). . . 127

6.2 Effects of spoofing attack in nominal conditions (the malicious attack begins at time $t = 70$ $[s]$ as highlighted by the vertical gray dash line). Maintaining tight formation maneuver under L-P-F topology: (a): time history of the position error computed as $r_i(t) - r_0(t) - d_{i0}$ ($\forall i = 1, \cdots, 7$); (b): time history of the speed error computed as $v_i(t) - v_0$ ($\forall i = 1, \cdots, 7$); (c): time history of the control effort $a_i(t)$ ($\forall i = 0, \cdots, 7$). 128

6.3 Spoofing attack (the malicious attack begins at time $t = 70$ $[s]$ as highlighted by the vertical gray dash line). Maintaining tight formation maneuver under L-P-F topology: (a): time history of the position error computed as $r_i(t) - r_0(t) - d_{i0}$ ($\forall i = 1, \cdots, 7$); (b): time history of the speed error computed as $v_i(t) - v_0$ ($\forall i = 1, \cdots, 7$); (c): time history of the control effort $a_i(t)$ ($\forall i = 0, \cdots, 7$). . . 129

6.4 Effects of spoofing attack in nominal conditions (the malicious attack begins at time $t = 70$ $[s]$, as highlighted by the vertical gray dash line). Maintaining tight formation maneuver under BR topology: (a): time history of the position error computed as $r_i(t) - r_0(t) - d_{i0}$ ($\forall i = 1, \cdots, 7$); (b): time history of the speed error computed as $v_i(t) - v_0$ ($\forall i = 1, \cdots, 7$); (c): time history of the control effort $a_i(t)$ ($\forall i = 0, \cdots, 7$). The symbol $'*'$ indicates the time instant when vehicles collide. 131

6.5 Spoofing attack (the malicious attack begins at time $t = 70$ $[s]$, as highlighted by the vertical gray dash line). Maintaining tight formation maneuver under BR topology: (a): time history of the position error computed as $r_i(t) - r_0(t) - d_{i0}$ ($\forall i = 1, \cdots, 7$); (b): time history of the speed error computed as $v_i(t) - v_0$ ($\forall i = 1, \cdots, 7$); (c): time history of the control effort $a_i(t)$ ($\forall i = 0, \cdots, 7$). . . 132

6.6 Effects of message falsification attack in nominal conditions (the malicious attack begins at $t = 70$ $[s]$ as highlighted by the vertical gray dash line). Maintaining tight formation maneuver under L-P-F topology: (a): time history of the position error computed as $r_i(t) - r_0(t) - d_{i0}$ $(\forall i = 1, \cdots, 7)$; (b): time history of the speed error computed as $v_i(t) - v_0$ $(\forall i = 1, \cdots, 7)$; (c): time history of the control effort $a_i(t)$ $(\forall i = 0, \cdots, 7)$. 133

6.7 Message falsification attack (the malicious attack begins at $t = 70$ $[s]$ as highlighted by the vertical gray dash line). Maintaining tight formation maneuver under L-P-F topology: (a): time history of the position error computed as $r_i(t) - r_0(t) - d_{i0}$ $(\forall i = 1, \cdots, 7)$; (b): time history of the speed error computed as $v_i(t) - v_0$ $(\forall i = 1, \cdots, 7)$; (c): time history of the control effort $a_i(t)$ $(\forall i = 0, \cdots, 7)$. . . 134

6.8 DoS attack (the malicious attack begins at $t = 2$ $[s]$ with a time duration of 20 $[s]$ and it is then repeated in a periodic fashion every 25 $[s]$ as highlighted by the vertical gray dash lines). Maintaining tight formation maneuver under L-P-F topology: (a): time history of the position error computed as $r_i(t) - r_0(t) - d_{i0}$ $(\forall i = 1, \cdots, 7)$; (b): time history of the speed error computed as $v_i(t) - v_0$ $(\forall i = 1, \cdots, 7)$; (c): time history of the control effort $a_i(t)$ $(\forall i = 0, \cdots, 7)$. 135

6.9 Burst attack (the malicious attack begins at time $t = 3$ $[s]$ as highlighted by the vertical gray dash line). Maintaining tight formation maneuver under L-P-F topology: (a): time history of the position error computed as $r_i(t) - r_0(t) - d_{i0}$ $(\forall i = 1, \cdots, 7)$; (b): time history of the speed error computed as $v_i(t) - v_0$ $(\forall i = 1, \cdots, 7)$; (c): time history of the control effort $a_i(t)$ $(\forall i = 0, \cdots, 7)$. 136

6.10 Radio Jamming attack (the malicious attack begins at time $t = 1$ $[s]$ with a time duration of 5 $[s]$ and it is then repeated in periodic fashion every 20 $[s]$ as highlighted by the vertical gray dash lines). Maintaining tight formation maneuver under L-P-F topology: (a): time history of the position error computed as $r_i(t) - r_0(t) - d_{i0}$ $(\forall i = 1, \cdots, 7)$; (b): time history of the speed error computed as $v_i(t) - v_0$ $(\forall i = 1, \cdots, 7)$; (c): time history of the control effort $a_i(t)$ $(\forall i = 0, \cdots, 7)$. 137
6.11 Leader tracking maneuver under L-P-F topology. Time history of vehicles speed, $v_i(t)$ $(\forall i = 0, \ldots, 7)$: (a): spoofing attack; (b): message falsification attack; (c): DoS attack; (d): burst attack. The vertical gray dash lines indicate the time instant when a malicious attacks begins. 139

7.1 A possible traffic junction scenario ($\mu = 4$). Vehicles cooperate for autonomously and exclusively crossing the Conflicting Area (CA). Once inside the Cooperative Zone (CZ), the vehicle i chooses one of the possible trajectories $t_{i,pq}$ starting from the road p where they are initially located. 144
7.2 Autonomous vehicles approaching the traffic junction as a virtual platoon problem w.r.t. the position from the centre of the chosen trajectory $p_i(t)$. a) Computation of the $p_i(t)$. b) Virtual platoon recast and choice of the desired distance according to Algorithm 2. 145
7.3 Four autonomous vehicles negotiating a six roads intersection $(i = 1, \ldots, 4)$. a) Time history of vehicles positions (boundaries of the CA: dash-dots horizontal lines). b) Time history of vehicle velocity. c) Time history of vehicles accelerations. d) Time history of position errors computed as $p_i(t) - p_j(t) - p^{\star}_{ij}$, $(i, j = 1, \ldots, 4\ i \neq j)$. e) Time history of the speed errors computed as $v_i(t) - v_j(t)$, $(i, j = 1, \ldots, 4\ i \neq j)$. Vertical lines in figures b), c) d) and e) indicate the time instant at the witch each vehicle enters and exits the CA. Note that the different colors refer the different vehicles (some vertical line are not visible since they are overlapped) 150
7.4 Settling time T [s] v.s. control gain $\alpha \in (0; 1)$. 151

8.1 Test Car Volvo XC90: a) front perspective; b) back perspective. 154
8.2 Test Car Volvo XC90 a) Test Car Volvo XC90 - External Instrumentation b) Test Car Volvo XC90 - Internal Instrumentation 155
8.3 Software architecture executed on OpenDLV. 156
8.4 Volvo Truck FH16 158
8.5 Test Truck Volvo FH16 - Instrumentation 158
8.6 Volvo Car S90 159
8.7 Volvo Car S90: ADB Pedal Robot 159
8.8 Test Car Volvo S90 Instrumentation 160
8.9 Software architecture executed on dSpace MicroAutobox. 160
8.10 The City Area at AstaZero 162
8.11 Map of the City Area at AstaZero 162
8.12 Experimental Test-05-th June 2018 164
8.13 Three autonomous vehicles scenario experimental results: a) time history of vehicles positions (boundaries of the CA: dash-dots horizontal lines); b) time history of vehicles velocities; c) time history of vehicles accelerations; d): 2nd vehicle position w.r.t. 1st and 3rd vehicle positions. 165
8.14 Three autonomous vehicles scenario experimental results: a) time history of position errors computed as $e_{ij} = p_i(t) - p_j(t) - p_{ij}^{\star}$ $(i, j = 1, \ldots, 3\ j \neq i)$; b): time history of the speed errors computed as $v_{ij}(t) = v_i(t) - v_j(t)$ $(i, j = 1, \ldots, 3\ j \neq i)$. 166
8.15 Two autonomous vehicles with one human-driven vehicle scenario. Experimental results: a) Time history of vehicles positions (boundaries of the CA: dash-dots horizontal lines). b) Time history of vehicles velocities. c) Time history of vehicles accelerations. 167

List of Tables

4.1 NETWORK SIMULATION PARAMETERS. 77
4.2 TRAFFIC SIMULATION PARAMETERS. 77

6.1 NETWORK SIMULATION PARAMETERS. 124
6.2 TRAFFIC SIMULATION PARAMETERS. 124

7.1 SIMULATION PARAMETERS 149

8.1 EXPERIMENTAL SCENARIOS PARAMETERS. 163

CHAPTER 1

Introduction

1.1 Motivation and Contributions

Connected autonomous vehicles have recently attracted extensive research interest due to its potential to benefit the road traffic significantly, e.g. enhancing road safety, improving traffic capacity and smoothness, and reducing fuel consumption [191, 57, 122, 126, 130]. The fundamental aim is to cooperatively drive the road by operating vehicles platoon that maintain an optimal inter-vehicular spacing policy, tracking at the same time desired speed and acceleration profiles. In this driving paradigm all connected vehicles embed wireless communication hardware in order to share information with neighbors and to receive the reference signal coming from the leading vehicle. To support Intelligent Transportation System (ITS) applications, both the Wi-Fi networks, based on IEEE 802.11p communication standard protocol [6], and the mobile network 4G/5G [35] are exploited. On the basis of information received from vehicles within the platoon, the on-board control algorithm is responsible of the safe tracking of the desired velocity and acceleration profile, i.e. vehicles have to track the leader motion, while respecting at the same time a pre-determined inter-vehicles spacing policy [8, 14].
Formation control of autonomous connected vehicles is one of the typical problems addressed in the general context of networked control systems (e.g. see [162, 59, 170, 174, 167, 111, 151, 60, 92] and references therein). By leveraging this paradigm, a platoon composed by multiple connected

and automated vehicles is represented as one-dimensional network of dynamical agents, in which each agent only uses its neighboring information to locally control its motion, while it aims to achieve certain global coordination with all other agents[155].
Within this theoretical framework, control algorithms are traditionally designed based on an implicit assumption of unlimited bandwidth and perfect communication environments [68]. However, in practice, communication resources are limited and not perfect. Indeed, wireless communications, enabling the cooperative driving applications, introduce unavoidable communication impairments such as transmission delay and packet losses that strongly affect the performances of cooperative driving [30, 218]. Communication time-delay and other networked-induced phenomena are hence crucial in cooperative driving application since they may lead the vehicular network to instability. Therefore, for the practical implementation of distributed strategies, they have to be taken into account from the beginning of the control design phase and the challenge in the control field is hence to design cooperative control algorithms that are resilient and robust to communication impairments.
This problem has been tackled in the current literature under the restrictive assumption that the communication delay is unique (or homogeneous, uniform, identical as indifferently referred in the technical literature) and often constant (see e.g. [135, 139, 86, 90, 182, 91, 123]).
However, when treating with communication networks, each communication link, that connects a pair of vehicles, is affected by a different variable time-delay that depends from actual conditions, or possible impairments, of the communication channel. It follows that the hypothesis commonly made in the technical literature of a unique and constant network delay may result unrealistic and that delays, affecting the outdated information that are used to compute the control input, have to be considered as a multiple time-varying functions depending from the specific communication link under investigation [153]. Indeed, time-delay itself might obey its own dynamics, which possibly depend on the communication distance, total computation load and computation capability.
Moreover, in addition to this problem, wireless communication networks can suffer different security threats. In collaborative driving applications, the sudden appearance of a malicious attack can mainly compromise: i) the correctness of data traffic flow on the vehicular network by sending

malicious messages that alter the platoon formation and its coordinated motion; ii) the safety of platooning application by altering vehicular network communication capability. In view of the fact that cyber attacks can lead to dangerous implications for the security of autonomous driving systems, it is fundamental to consider their effects on the behavior of the interconnected vehicles, and to try to limit them from the control design stage. Past studies on wireless communication networks security vulnerabilities focus their attention on an accurate classification of malicious attacks and the solutions to mitigate them at communication level [4]. However, while security in sensing and communication has been extensively investigated in the technical literature, security in control has been recently indicated as a key ingredient that has to be added for enhancing the protection level of the normal operation of a physical process [75, 124].
From control viewpoint, recent literature on the security of the networked cyber-physical systems is usually devoted to designing state estimators for the better understanding of system dynamical behaviors and the attack detection (see survey [50] and references therein). The exploitation of the cooperation property of the networked control systems paradigm, or more precisely the exploitation of all information exchanged among the agents within the networked control system, could be also a promising solution so to counteract security vulnerabilities [151]. However, many issues are still open, as for example the need of designing distributed control protocols able to cope simultaneously with network induced phenomena - such as the unavoidable delays that affect in practice the information shared via a wireless channel - and different kinds of possible cyberattacks [50].
Hence, from the literature overview on cooperative driving control strategies, and more in general on the networked control systems, the following main challenges arise:

1. Designing distributed cooperative control algorithms that are resilient and robust to multiple time-varying communication delays and packet losses.

2. Designing resilient secure distributed control algorithms able to counteract different security vulnerabilities when considering the wireless communication network non-ideal.

The aim of this thesis is to tackle and solve both the challenges by proposing different properly designed control strategies. Specifically, for dealing with the challenge 1 a novel adaptive distributed cooperative approach is proposed so to achieve the cooperative driving despite the presence of communication delays, assumed to be heterogeneous (multiple) and time-varying. The proposed control strategy updates its action on the basis of state errors among the vehicle itself and the delayed state information received from neighboring vehicles through the wireless communication network. On-board controllers, that automatically compensates the outdated information caused by network delays, compute a not-identical control input since different adaptive gains are associated to each communication link. The adaptive approach has been chosen since it provides robustness with respect to unmodeled dynamics and uncertain parameters [193, 154], so to better counteract the effects of all disturbances that always characterize real vague environments. To disclose this aspect a detailed robustness analysis w.r.t. external disturbances is also provided. The stability of the adaptive strategy is analytically proven by exploiting the Lyapunov-Krasovskii method and the stability criterion is expressed as a Linear Matrix Inequalities (LMIs) whose solution also provides the estimate of the delay margin that guarantees stability. The effectiveness of the proposed strategy is shown by using PLEXE[169, 170, 167], a state of the art inter-vehicular communications and mobility simulator that includes basic building blocks for platooning.
Again for addressing the challenge 1, we also propose a nonlinear finite controller for the specific cooperative driving applications of autonomous vehicles approaching the traffic junction. The crossing problem is recast as the control of a virtual longitudinal platoon that opportunely arranges the vehicles that may be in different lanes of the junction and may have different directional intentions. Specifically, this recast has been proposed in the seminal work [188] and recently exploited in [132], where a just simulation study shows the performance of a classical longitudinal (virtual platooning) controller based on a linear CACC strategy which is essentially an inter-vehicle distance control algorithm that ensures the string stability, i.e. ensures that once at steady-state, the inter-vehicular distances are kept constant. However, for safety reasons, a fundamental problem is to guarantee, besides the robustness to communication impairments, from the very beginning of control design, that the desired virtual

formation is effectively reached before vehicles enter the Conflicting Area (CA), i.e. the intersection core area where collisions could occur. To face this issue, a completely distributed nonlinear finite-time control strategy for cooperative vehicles negotiating an intersection is proposed. Collisions are, hence, prevented due to the achievement of the desired virtual formation in a finite time T before the first vehicle accesses the CA. Moreover, the control protocol guarantees desired inter-vehicle distances among virtual platoon members such that real vehicles access the CA in a mutually exclusive fashion, while the simultaneous achievement of a common platoon velocity ensures that the desired formation will be preserved once reached. The stability analysis is an on-going work and its effectiveness is validated in numerical and experimental way.
For dealing with the challenge 2 we propose a novel distributed collaborative strategy that guarantees the platoon formation in adversarial environment and that allows to promptly react to security vulnerabilities such as messages manipulation attacks and communication capability attacks. The proposed distributed control approach also leverages a real-time voting technique to achieve the complete mitigation of some of the most critical effects due to malicious attacks. This does not imply that we aim to substitute other solutions for security, such as the cryptographic ones [121] that work at the information level to avoid that the content of the information can be somehow altered. Our aim is to provide further countermeasures to detect, mitigate and, if possible, counteract cyber threats that may alter driving decision at control level so to help increasing the overall security of the ensemble of the connected vehicles. The stability of the proposed secure control strategy is demonstrated by exploiting the Lyapunov-Krasovskii theory and an extensive simulation analysis discloses the effectiveness, the robustness and resiliency of the proposed approach and its capabilities in reacting to the malicious attack effects.
Some of the proposed cooperative driving control strategies have been also experimentally validated during on the road tests that have been carried out at the AstaZero test track near Gothenburg (Sweden) and have involved three vehicles properly equipped for autonomous driving and connected via wireless communication network. Specifically the experimental tests refer to the cooperative crossing problem of autonomous vehicles approaching a traffic junction and sharing information via 5G

mobile communication network. Experimental results indicate that the proposed approach is effective in guaranteeing the safe crossing in real on-the-road scenarios. Note that, with no loss of generality, the presented experimental setup can be easily used also for testing all the control strategies proposed in this thesis.

1.2 Thesis Outline

The thesis is structured as follows.

- In Chapter 2 some useful concepts and definitions are summarized for the sake of clarity.
- In Chapter 3, after presenting the cooperative driving systems, we describe how to model them as networked control systems. Moreover, we highlight the open control problems both in cooperative driving application field and in the general context of networked control systems.
- In Chapter 4 we solve the cooperative driving problem by proposing a novel distributed adaptive synchronization-based control strategy able to effectively operate on information, exchanged via vehicular networks, despite the presence of unavoidable communication impairments, such as multiple time-varying delays (that affect communication links) and packet losses. Herein, we analytically demonstrate the convergence of the control approach via a Lyapunov-Krasovskii approach. The effectiveness of the proposed strategy is shown via an extensive numerical simulations in PLEXE. Note that the content of this chapter has been presented in [155].
- In Chapter 5 we study the robustness property of the adaptive control protocol proposed in Chapter 4 in counteracting both multiple time-varying communication delays and external disturbances. The robust stability is proven via the Lyapunov-Krasovskii theory. Delay-dependent LMIs conditions are analytically derived for ensuring both robust synchronization to the leader dynamics and disturbances attenuation. An exemplar simulation result discloses the effectiveness of the approach. Note that the content of this chapter has been presented in [48].

- In Chapter 6 we focus on some relevant types of malicious threats that affect the platoon safety, i.e. application layer attacks (Spoofing and Message Falsification) and network layer attacks (Denial of Service and Burst Transmission), and we propose a novel collaborative consensus-based control strategy for enhancing the protection level of autonomous platoons and hence counteracting them. The control protocol stability is analytically demonstrated via the Lyapunov-Krasovkii approach and numerically validated via PLEXE simulator. Note that the content of this chapter has been presented in [152].

- In Chapter 7 we focus on cooperative driving control of autonomous vehicles approaching a traffic junction. The cooperative crossing application is addressed by recasting the intersection geometry as a virtual platoon and solved by leveraging a distributed finite-time controller that exploits outdated information, shared via the brand new 5G communication network, to proper compute its action. The stability of the closed-loop is an on-going work and hence not reported in this thesis. Numerical simulations disclose the effectiveness of the control approach in guaranteeing the cooperative crossing of autonomous vehicles at traffic junction without collisions.

- In Chapter 8 an overview of the experimental setup, composed of three prototype vehicles and used to validate some of the proposed cooperative driving control strategy, is presented; details on both the hardware and software solutions are provided. Specifically, the experimental tests refer to the cooperative crossing problem presented in Chapter 7. The experimental results achieved during the on the road tests at AstaZero confirm the effectiveness of the strategy in guaranteeing the safe crossing in real on-the-road scenarios.

- In Chapter 9 conclusions are drawn.

CHAPTER 2

Mathematical preliminaries and Background

2.1 Cooperative Control of networked dynamical systems

Networked dynamical systems consist of groups (i.e. ensemble) of dynamical systems exchanging their information and interacting with each other through wireless/wired communication networks, in order to agree, for example, upon a certain quantity of interest. Many real systems in nature and human society can be modeled as networked dynamical systems thus in the last two decades cooperative systems have received a compelling attention in different research fields such as physics sciences, mathematics, economic science and engineering [183]. Many researchers, inspired by natural occurrence of flocking and formation forming, have focused their work on synchronization, consensus and coordination of networked dynamical systems [86, 118], i.e. in controlling the whole network in order to produce a common behavior by applying distributed algorithms and to guarantee a smart group behavior. Examples in engineering deal with the coordinated motion of autonomous vehicles [163, 170, 169, 167, 151, 60], the phase or frequency synchronization in power grids [166, 51], and the synchronization of

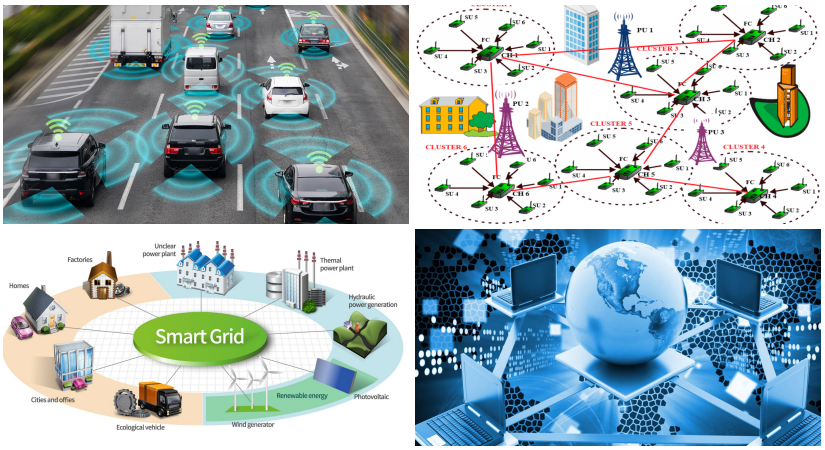


Figure 2.1: Example of networked dynamical systems in engineering.

wireless sensor networks [181, 210] (see Fig. 2.1).

2.1.1 Networked Dynamical systems Modeling

Basically, to model the networked dynamical systems we have to define:

1. A model of each dynamical system within the network, called agent or node;
2. The interaction protocol between agents;
3. The structure of the communication which indicates how and if an agent obtains information about other agents depending on the active communication links.

Each agent can be thought of as a generic non-linear control system of the form:

$$\dot{x}_i(t) = f_i(x_i(t)) + g_i(x_i(t))u_i(t), \tag{2.1}$$

with $x_i(t) \in \mathcal{R}^n$ and $u_i(t) \in \mathcal{R}^m$.
The interaction between agents can be modeled by choosing an appropriate coupling law. For example, the coupling between nodes can be

modeled as:

$$u_i(t) = \sigma \sum_{j=1, j\neq i}^{N} \alpha_{i,j} h(x_i(t), x_j(t)), \tag{2.2}$$

where σ is the coupling gain, $\alpha_{i,j}$ model the presence/absence of coupling between agents in the network and $h(x_i(t), x_j(t))$ refers to the particular protocol used.
The communication structure is modeled by a graph where every agent is a node and every communication link connecting a pair of agents is an edge. Hence a network of N dynamical agents is modeled as an N-order graph $\mathcal{G} = (\mathcal{V}, \mathcal{E})$ where $\mathcal{V}$ is the set of nodes and $\mathcal{E}$ is the set of edges [189]. There are different ways to characterize mathematically a network [69]. One of these representation is given by *adjacency matrix*. The adjacency matrix $\mathcal{A}$ is a matrix whose elements are 1 if and only if exists an edge from vertex i to vertex j. Consider an undirected network $\mathcal{G} = (\mathcal{V}, \mathcal{E})$ with N vertices, and let's label the vertices with integer labels $(1, ..., N)$. If we denote an edge between vertices i and j by (i, j) then the complete network can be specified by the matrix $\mathcal{A} \in \mathcal{R}^{N\times N}$, whose elements are so defined:

$$\alpha_{i,j} = \begin{cases} 1 & if : (i,j) \in \mathcal{E} \\ 0 & otherwise \end{cases} . \tag{2.3}$$

In some situations, however, it is useful to represent edges as having a strength, weight, or value to them, usually a real number. Thus in the Internet, for example, edges might have weights representing the amount of data flowing along them or their bandwidth. In this case we speak about weighted networks and the adjacency matrix will not have only elements equal to 1 or 0. Furthermore we can speak about delayed networks if the communication between agent i.e. each link of the network, is affected by a time-delay even though the agent is characterized by an own non delayed dynamics. To characterize analytically this situation, it is possible to define for each edge $(i, j) \in \mathcal{E}$ a function $\tau_{i,j}(t)$ that model the communication delay among the agent i nd the agent j. Indeed the assumption that there exist a communication time-delay between agent is a very realistic assumption for many real system as the World Wide Web. In reality the communication is not instantaneous, but the exchanged information is affected by a time-delay although sometimes

negligible. For every node $v_i \in \mathcal{V}$, we can define the set of neighbours N_i as the subset of $\mathcal{V}$ defined as follow:

$$N_i = \{j \in V : \alpha_{i,j} \neq 0\}. \tag{2.4}$$

The degree of a vertex in a graph is the number of edges connected to it. We will denote the degree of vertex i by Δ_i. In general Δ_i is so calculated:

$$\Delta_i = \sum_{j=1, j\neq i}^{N} \alpha_{i,j}. \tag{2.5}$$

Furthermore we can define the diagonal matrix $\Delta \in \mathcal{R}^{N\times N}$ whose diagonal element are the vertex degrees:

$$\Delta = \begin{bmatrix} \Delta_1 & 0 & ... & 0 \\ 0 & \Delta_2 & ... & 0 \\ ... & ... & ... & ... \\ 0 & 0 & ... & \Delta_n \end{bmatrix}. \tag{2.6}$$

Thanks to the degree matrix Δ and to the adjacency matrix $\mathcal{A}$, we can define an another important matrix, called Laplacian matrix $L \in \mathcal{R}^{N\times N}$.

$$L = \Delta - \mathcal{A} \tag{2.7}$$

For construction, the Laplacian matrix has zero row-sum, hence, at least one eigenvalue will be zero.

2.1.1.1 Digraph Propriety

A directed network or directed graph, also called a *digraph* for short, is a network in which each edge has a direction, pointing from one vertex to another. Such edges are themselves called directed edges, and can be represented by lines with arrows on them. Example of directed network is the World Wide Web, in which hyper-links run in one direction from one web page to another. Conversely a graph is defined undirected if each edge has not a direction. A digraph is strongly connected if there is a path from every node to every other node. A strong component of a digraph is an induced subgraph that is maximal, which is subject to being strongly connected. A directed tree is a digraph in which every

node has exactly one parent node with the exception of one node, which is called the root, which has no parent and has a directed path to every other node. We say that j is reachable from node i if there exists a path from node i to node j. A node is said to be globally reachable if it is reachable from any other node in the graph. In the case of undirected graph the Laplacian matrix is a symmetric matrix with zero row-sum and real spectrum. For a digraph the Laplacian matrix is so defined:

$$L = [l_{i,j}] = \begin{cases} l_{i,i} = \sum_{j=1, j\neq i}^{N} \alpha_{i,j} \\ l_{i,j} = -\alpha_{i,j} \qquad i \neq j \end{cases} \tag{2.8}$$

2.1.2 Consensus and Synchronization in networked dynamical systems

In networks of agents (or dynamical systems), consensus means to reach an agreement regarding a certain quantity of interest that depends on the state of all agents. A consensus algorithm (or protocol) is an interaction rule that specifies the information exchange between an agent and all of its neighbours on the network [143]. Every agent exploit the same algorithm and take decision thanks to the local available information and those that receive from the other agents.
Consider a network of agents interested in reaching a consensus via local communication with their neighbours on a graph $\mathcal{G} = (\mathcal{V}, \mathcal{E})$ that represent the agent connection. By reaching a consensus, we mean asymptotically converging to a constant agreement value, i.e.:

$$\lim_{t \longrightarrow \infty} x_i(t) = \bar{x} \ \forall i \in \mathcal{V} \tag{2.9}$$

being $\bar{x}$ the collective decision of the group.
Most early papers on networked dynamical systems address consensus problem without considering the presence of a leader node, so all nodes are commanded to converge toward a not prescribed common evolution. Synchronization, in the sense of cooperative tracking, has been then studied by adding a leader that imposes the desired behavior to a group of agents to achieve the command trajectory (e.g., see [205], [119] and

references therein). According to [112], we say that the networked dynamical systems achieve synchronization if

$$\lim_{t\to\infty} \|x_i(t) - x_0(t)\| = 0, \quad i = 1, \dots N, \tag{2.10}$$

where $x_i = (x_{i1}, x_{i2}, \dots, x_{in})^T \in \mathbb{R}^n$ are the state variables of node i and $x_0 = (x_{01}, x_{02}, \dots, x_{0n})^T \in \mathbb{R}^n$ are the reference state variables of the leader node. The hyperplane:

$$\mathcal{S} = \left\{ \left[x_1^\top(t), x_2^\top(t), ..., x_N^\top(t) \right]^\top \in \mathcal{R}^{N\times N} : x_i(t) = x_j(t) = x_0(t) \right\}$$

for $i, j = 1, 2, ..., N$ is said to be the synchronization manifold of the networked dynamical systems.

2.2 Stability of Continuos-Time Systems

In what follow some useful results about stability of linear system are recalled. We begin by considering the familiar linear state equation:

$$\dot{x}(t) = Ax(t). \tag{2.11}$$

For this class of systems, the following result hold:

Theorem 1. *(Lyapunov stability for linear systems) Consider a linear system in the form of (2.11) and let $A \in \mathcal{R}^{N\times N}$. The following statements are equivalent:*

- *all the eigenvalues of A have negative real part;*
- *for all matrices $Q = Q^\top > 0$ there exists an unique solution $P = P^\top > 0$ to the following (Lyapunov) equation:*

$$AP^\top + PA = -Q \tag{2.12}$$

Consider now, a time varying linear system in the form:

$$\dot{x}(t) = A(t)x(t), \tag{2.13}$$

for $A \in \mathcal{R}^{N\times N}$ and $t \in \mathcal{R}$. Without loss of generality, assume that Eq. (2.13) has equilibrium $x = 0$. To establish asymptotic stability

of this equilibrium, a standard approach is to seek standard quadratic Lyapunov function associated with Eq. (2.13). A typical choice is the classical quadratic function $V(x(t)) = x(t)^\top Px(t)$. Evaluating the time derivative $\dot{V}(t)$ along the system trajectory we have:

$$\dot{V}(x(t)) = x(t)^\top \left[A(t)^\top P + PA(t)\right] x(t), \tag{2.14}$$

and thus it is sufficient to seek a matrix $P \in \mathcal{S}_n^+$ which satisfies the continuous-time algebraic Lyapunov equation:

$$A(t)^\top P + PA(t) = -M(t), \tag{2.15}$$

where $M(t) \in \mathcal{S}_n^+$ is given. Here, $\mathcal{S}_n^+$ denotes the set of real, $n \times n$ positive definite symmetric matrices.

Theorem 2. *[42] The unique solution of Eq.* (2.15) *is given by:*

$$P = \int_{t_0}^{\infty} \phi_A^\top(s, t_0) M(t) \phi_A(s, t_0) ds, \tag{2.16}$$

where $\phi_A(t, t_0)$ is the transition matrix for the system Eq. (2.13)*. Moreover, $P \in \mathcal{S}_n^+$ whenever $M(t) \in \mathcal{S}_n^+$*

On the other hand, suppose we seek a Lyapunov function of the form $V(x(t)) = x(t)^\top P(t)x(t)$, the emphasis being that P is time varying. Then

$$\dot{V}(x(t)) = x(t)^\top \left[A(t)^\top P(t) + P(t)A(t) + \dot{P}(t)\right] x(t), \tag{2.17}$$

and so we seek a $P(t) \in \mathcal{S}_n^+$ which satisfies the continuous-time differential Lyapunov equation

$$A(t)^\top P(t) + P(t)A(t) + \dot{P}(t) = -M(t), \tag{2.18}$$

where $M(t) \in \mathcal{S}_n^+$ is specified.

Theorem 3. *[42] The unique solution of Eq.* (2.18)*, subject to the initial condition $P(t_0) = P_0$ is given by:*

$$P(t) = \phi_A^{-\top}(t, t_0) P(t_0) \phi_A^{-1}(t, t_0) - \int_{t_0}^{\infty} \phi_A^\top(s, t_0) M(t) \phi_A(s, t_0) ds \tag{2.19}$$

where $\phi_A(t, t_0)$ is the transition matrix for the system Eq. (2.13)*. Moreover, $P \in \mathcal{S}_n^+$ whenever $M(t) \in \mathcal{S}_n^+$*

2.3 Time-Delay Systems Theory

Time delay systems are systems in which a significant time delay exists between the applications of input to the system and their resulting effect. Such systems arise from an inherent time delay in the components of the system or from a deliberate introduction of time delay into the system for control purposes. Such time delay systems can be represented by delay differential equations, which belong to the class of functional differential equations [203]. The analysis of time-delay systems is a well-developed field gathering a lot of different techniques. These methods can be categorized to either belong to frequency-domain or time-domain techniques. Frequency-domain approaches are mostly devoted to linear time-invariant systems, yet under some circumstances, it is possible to adapt them to address the case of varying delays using, for instance, model transformations. Time-domain approaches can, however, be applied to any type of systems: linear or non-linear, with constant or time-varying delays, etc. [28]. Most of the existing results for stability of systems with time-varying delays, based on time-domain approaches, are developed based on the following two Lyapunov-type approaches [100]:

- The *Lyapunov-Razumikhin* method that looks for functions which normally allow one to prove stability of systems with bounded but freely fast time-varying delays. See for example papers [29] and [117].

- The *Lyapunov-Krasovskii* method that looks for functionals which only allow one to prove stability of time-delay systems where the delay parameters are bounded both in length and time variation ([64, 80, 108, 133, 105]). In [64], a discussion about the conservatism among the different methods is given.

The main difference among the two approach relies int the fact that Razumikhin gives more conservative bound on the maximum allowable delay preserving stability than the Lyapunov-Krasovskii approach, as showed in [74].

2.3.1 Krasovskii theorem

In what follows we provide some definitions and results on the stability of delayed systems, according to Lyapunov-Krasovskii theory.

Definition 1. *(Uniform norm) Let $\phi(s) \in \mathcal{C}([a,b],\mathbb{R}^n)$ be the set of continuous functions mapping the interval $[a,b]$ to $\mathbb{R}^n$, then the uniform norm of ϕ is defined as*

$$\|\phi\|_{\mathcal{C}} = \max_{a\leq s\leq b} \|\phi(s)\|. \tag{2.20}$$

In this definition, the vector norm $\|\cdot\|$ represents the $2-$norm $\|\cdot\|_2$.
We use functional differential equations to describe time-delay systems. The general form of a retarded functional differential equation (RFDE) (or functional differential equation of retarded type) is:

$$\begin{aligned} \dot{x}(t) &= f(t, x_t),\ t \geq t_0 \\ x(t_0 + s) &= \phi(s),\ s \in [-h, 0] \end{aligned} \tag{2.21}$$

where $h > 0$ is the delay and $\phi \in \mathcal{C}([-h,0],\mathbb{R}^n)$ is the functional of initial conditions. The state of the system $x_t \in \mathcal{C}([-h,0],\mathbb{R}^n)$ is defined as $x_t(\theta) = x(t+\theta)$. Moreover, $x_t(t_0,\phi)$ denotes the state-value at time t with initial condition $x_{t_0} = \phi$.
For the class of systems in (2.21) it holds the following theorem:

Theorem 4. *(Lyapunov-Krasovskii Stability Theorem) [72] Suppose that $f : \mathbb{R}_{\geq t_0} \times \mathcal{C}([-h,0],\mathbb{R}^n) \to \mathbb{R}^n$ given in (2.21) maps $\mathbb{R}_{\geq t_0}\times$ (bounded sets of $\mathcal{C}([-h,0],\mathbb{R}^n)$) into a bounded sets of $\mathbb{R}^n$, and that $u, v, w : \mathbb{R}_{\geq 0} \to \mathbb{R}_{\geq 0}$ are continuous non-decreasing functions, where additionally $u(s)$ and $v(s)$ are positive for $s > 0$, and $u(0) = v(0) = 0$. Assume further that there exists a continuous differentiable functional $V : \mathbb{R} \times \mathcal{C}([-h,0],\mathbb{R}^n) \to \mathbb{R}$ such that*

$$u(\|\phi(0)\|) \leq V(t,\phi) \leq v(\|\,\phi\|_{\mathcal{C}}) \tag{2.22}$$

and

$$\dot{V}(t,\phi) \leq -w(\|\phi(0)\|), \tag{2.23}$$

then the trivial solution of (2.21) is uniformly stable. If $w(s) > 0$ for $s > 0$, then it is uniformly asymptotically stable. In addition, if

$$\lim_{s\to\infty} u(s) = +\infty,$$

then it is globally uniformly asymptotically stable.

It is important to note that there exists two types of stability results, and can be be distinguished based on whether they depend on the delay value. In some cases it is possible to asses stability of delayed system for a range of delay values or even obtain stability results for family of delays. This leads us to the concepts of delay-independent and delay-dependent stability.

Definition 2. *(Delay-Independent Stability) [28] A time-delay system is stable independently of the delay or delay-independent stable if stability does not depend on the delay value, that is, if the system is stable for any delay value in* $[0, \infty]$.

The above definition immediately extends to systems with multiple delays and time-varying delays. This concept of stability is quite strong since delays must have no impact on stability. This imposes, in return, strong constraints on the structure of the system. It is therefore expected that time-delay systems are, most likely, not delay-independent stable.

Definition 3. *(Delay-Dependent Stability) [28] A time-delay system is delay-dependent stable if there exists a (bounded) interval* $I \in \mathcal{R}$ *for which the system is stable for any delay in* I*, and unstable otherwise.*

Unlike delay-independent stability, delay-dependent stability is a concept of stability that is actually sensitive to change in the delay values. This is certainly the most realistic notion of stability since delays are, most of the time, influential on the stability of real world systems.

2.3.2 Model transformation - Leibniz-Newton formula

Model transformation is a very common procedure introduced quite early in the analysis of time-delay systems, but not restricted to. The rationale behind model transformations is to turn a time-delay system into another system, referred to as a comparison system or comparison model, which may or may not be a time-delay system [28]. Analysis tools are then applied on the comparison system in order to draw conclusions on the stability of the original time-delay system. Model transformations lie at the core of many efficient analysis techniques such as Lyapunov-Razumikhin and Lyapunov-Krasovskii approaches. The goal of model transformations is to simplify the analysis of time-delay systems. The compensation for

this is that the comparison system may exhibit additional dynamics leading to a possible loss of equivalence, in terms of stability, between the original and the comparison system. Additional dynamics consist of supplementary zeros in the characteristic equation of the comparison model. When at least one of these additional zeros is unstable, the comparison model is unstable and the stability of the original system cannot be inferred from the comparison model [72]. Many different model transformation procedures have been proposed in the literature, however, in this thesis work we will exploit the Leibniz-Newton formula [28].

Definition 4. *(Newton-Leibniz transformation) [28] The Newton-Leibniz model transformation is based on the following identity:*

$$x(t-h) = x(t) - \int_{t-h}^{t} \dot{x}(s)ds \tag{2.24}$$

2.4 Integral inequalities

In this section, some integral inequalities, exploited during the dissertation, have been retrieved.
First of all we recall the Hadamard inequality, valid for convex functions only:

Lemma 1. *(Hadamard Inequality) [53] Let $f : I \subseteq \mathcal{R} \to \mathcal{R}$ be a convex mapping defined on the interval I of real numbers, then the following inequality holds:*

$$\frac{1}{b-a}\int_{a}^{b} f(x)dx \leq \frac{f(a)+f(b)}{2}, \tag{2.25}$$

being $a, b \in I$ with $a < b$.

The following integral inequality is known as the Jensen Inequality, which plays an important role in the stability problem of time-delay systems:

Lemma 2. *(Jensen Inequality) [72] For any constant matrix $\Theta = \Theta^{\top} > 0 \in \mathcal{R}^{N\times N}$, scalar $h : h(t) > 0$, and vector function $x(.) : [-h, 0] \longrightarrow \mathcal{R}^n$ such that the following integral is defined, then*

$$h\int_{t-h}^{t} \eta^{\top}(s)\Theta\eta(s)ds \geqslant \int_{t-h}^{t} \eta^{\top}(s)ds\Theta\int_{t-h}^{t} \eta(s)ds. \tag{2.26}$$

Moreover we recall the following useful integral inequality:

Lemma 3. *[89] For any generic positive definite matrix* Ξ *it holds*

$$2a^\top c \leq a^\top \Xi a + c^\top \Xi^{-1} c. \tag{2.27}$$

CHAPTER 3

Cooperative Driving of Autonomous Connected Vehicles as Networked Control Systems

3.1 Cooperative Driving Systems

Owing to the ever-increasing traffic demand, modern societies with well-planned road management systems, and sufficient infrastructures for transportation, still face the problem of traffic congestion. This results in loss of travel time, and huge societal and economic costs and an increasing environmental impact [17]. To give new answers to the increasing mobility demand and other open issues, several solutions have been adopted. Some of these rely on the enhancement or on the construction of new infrastructures (like roads, highways, port, airport and so on), some others rely on the enhancement of the vehicular safety systems (like air-bags or safety belt). However, it is clear that building new infrastructures require several expensive actions with the drawback of an increased environmental impact [61]. For this reasons, solutions allowing a more efficient use of the existing infrastructure are aimed. Intelligent

Transportation Systems (ITS) is a fairly new concept which gives a new vision of mobility that, thanks to the integration of Information and Communication Technologies (ICT) with traditional transport infrastructures, allows users to get more from transportation systems, in greater safety and with less environmental impact improving the overall efficiency. The idea of ITS, in road transports, rely on the possibility to connect among them vehicles with other vehicles or with central or de localized infrastructure, helping to find new solutions to problems like collision avoidance, fleet management, driver assistance etc. As depicted in Fig. 3.1, the goal thus became vehicles and infrastructure cooperate to perceive potentially dangerous situations in an extended space and time horizon [147]. Communication and cooperation between vehicles

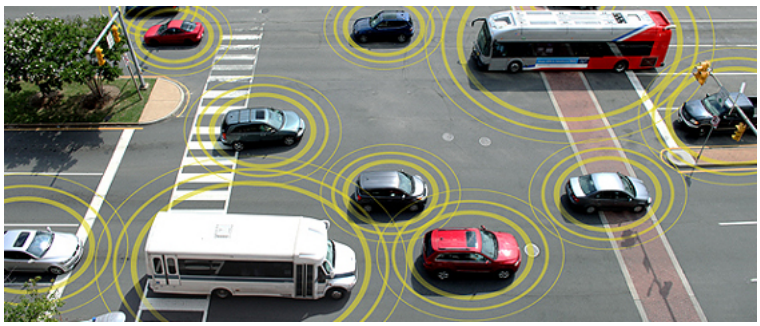


Figure 3.1: ITS scenario: Vehicles communicate information each other.

offer the opportunity to develop many different applications [31]:

- *safety applications*: which aim to mitigate vehicular collisions such as rear ending;
- *mobility applications*: which look at increasing traffic flow through information sharing about road conditions;
- *comfort applications*: such as cooperative adaptive cruise control, which aim at reducing the driver work load.

Among the the different ITS solution, we focus on Cooperative Driving Systems.
Cooperative driving systems exploit the wireless communication as an

additional sensor both to perceive the presence of neighboring vehicles and to communicate (e.g. in broadcast) their own presence and in vehicle data. The idea of vehicles cooperating via wireless communication dates back to the 1980s [140], when California PATH program was established to study and develop vehicle-highway cooperation and communication systems [8, 179]. The basic idea is to enable the communication and the cooperation among neighboring vehicles to safely reduce their mutual distance, hence increasing the road capacity, and suppress traffic shockwaves, hence reducing fuel consumptions [106].
To allow communication among nearby vehicles or between vehicles and nearby fixed roadside equipment, different architectural solution for creating vehicular networks were proposed. Such architectures have to guarantee two main communication paradigm:

- a pure wireless Vehicle-to-Vehicle (V2V), allowing vehicular communication with no infrastructure support;
- an hybrid Vehicle-to-Infrastructure (V2I) architecture that does not rely on fixed infrastructure in a constant manner, but can exploit it for improved performance and service access when it is available.

Actually the V2I architecture implicitly includes V2V communication. The communication between vehicles or between vehicles and road infrastructure enable vehicles and infrastructure to form a cooperative system where the users exchange information and cooperate to improve quality of travel experience. In *Cooperative Driving systems* vehicles are organized as a platoon, i.e. a set of vehicles that, in order to reach a common objective, share information about their state information (position, velocity, acceleration, consumption, emission etc.) or communicate with a road side infrastructure, through a wireless communication network such as 4-5G or WLANs IEEE 802.11a/b/g/p [83] (see Fig. 3.2). The core of such cooperative driving systems is a set of algorithms deployed on the vehicles and controlling their motion based on the behavior of the surrounding vehicles so to achieve an inter-vehicle separation (smaller than the one guaranteed by human drivers, but safe) while increasing road capacity and decreasing, at the same time, traffic congestion [81, 113, 38] Another benefit, originated by cooperation, is that the aerodynamic drag is reduced (especially for heavy-duty vehicles) thereby increasing fuel economy and, consequently, reducing pollutants

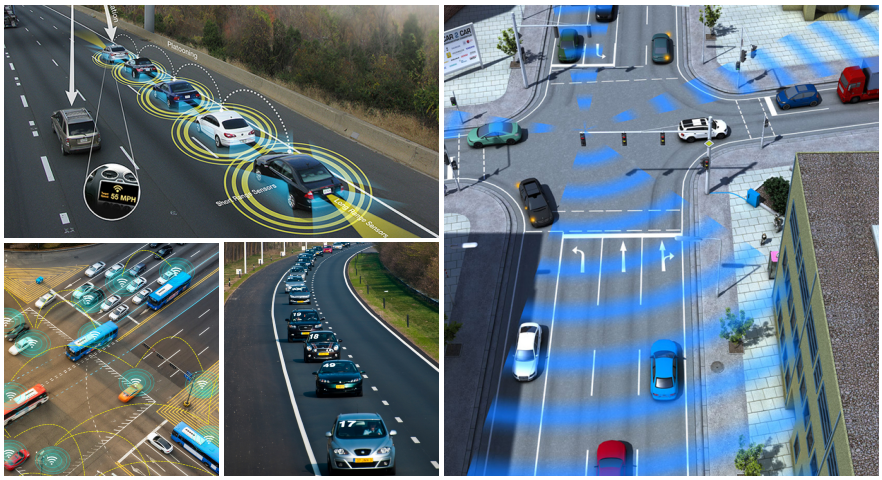


Figure 3.2: Cooperative driving systems.

emissions [136]. To achieve these objectives, the cooperative driving systems are characterized by distributed, hierarchical control, where the high level control structure takes decisions and compute set point for lower level controller that acts on the throttle and brake systems. As exemplary case we take the architecture shown in Fig. 3.3 [187], where is possible to distinguish three layers: the vehicle control layer and the vehicle management layer that are present on each vehicle, and the traffic management layer, common to all the vehicles and shared by them, that is on the infrastructure. The functions of the vehicle control layer are to sense the conditions and states ahead of the vehicle and to activate the lateral and longitudinal actuators. The layer outputs sensing data and vehicle state variables to the vehicle management layer and receives commands of the steering and vehicle speed from it. Each vehicle may have its individual vehicle control layer. The vehicle management layer determines the movement of each vehicle under the cooperative driving with the data from the vehicle control layer, those received from neighbouring vehicles through the inter-vehicle communications, and from the traffic control layer through the road-vehicle communications. The criteria of the movement comes from the traffic control layer. The traffic control layer has two parts: physical part, that includes the infrastructure-based ITS equipment like sign boards, traffic signals, and the road-vehicle communications, and a logical part that includes common sense, laws,

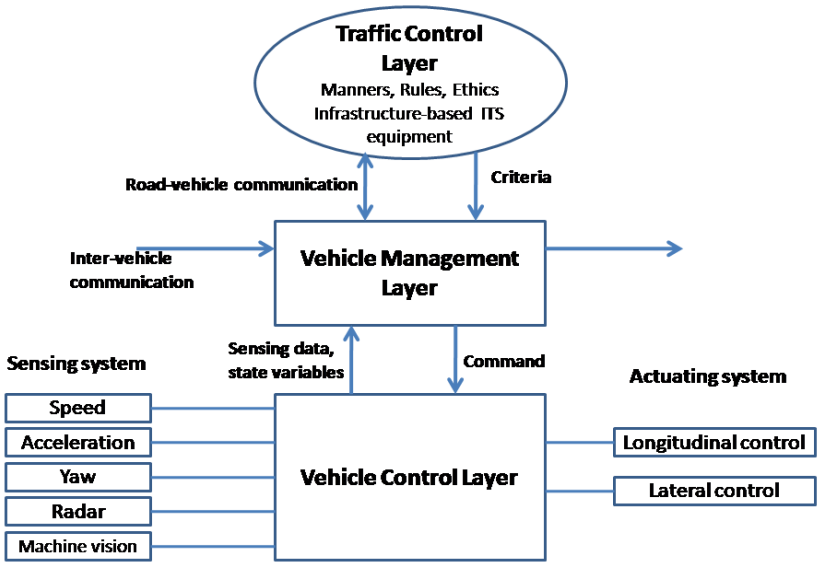


Figure 3.3: The architecture for the cooperative driving of automated vehicles.

rules, manners, and ethics in the human society. Within the two parts, a criteria that must be common to neighbouring vehicles will be found and sent to the vehicle management layer in each vehicle. The cooperative control strategies, that drives the collective behavior of vehicles platoon, are usually deployed on vehicle management layer and traffic control layer of the architecture in Fig. 3.3. The control strategy precursors of cooperative driving system, introduced by the automotive industry, is the Adaptive Cruise Control ACC system. The ACC is considered to be the successor of the conventional Cruise Control (CC). A vehicle with CC is able to maintain a pre-selected speed if no vehicle is up-front. The ACC is a radar-based system which is designed to enhance driving comfort and convenience by relieving the driver of the need to continually adjust his or her speed to match that of a preceding vehicle. The system slows down the speed when it approaches a vehicle with a lower speed and the system increases the speed to the level of speed previous set when the vehicle upfront accelerates or disappears (e.g. by

changing lanes) [190]. Recently, V2V communication have pushed the ACC system into a more sophisticate system, called CACC. Each vehicle within the cooperative driving system is equipped with on-board sensors measuring position, velocity, acceleration. Such set of measurements requires Inertial Measurements Units (IMU), Global Positioning Systems (GPS) and radars, which are commonly available on road vehicles. Each vehicle is also equipped with wireless V2V communication hardware to share information with its neighbors and receive reference signals. Thanks to the information of neighbors vehicles CACC controller will be able to anticipate problems better, enabling it to be safer, smoother and more reliable in response. In CACC, wireless communication is used by the controller to regulate speed and distance between vehicles, ensuring that any changes in speed by the driver in front of you are immediately registered in the cooperative vehicle. However, most of the CACC controller presented in literature does not cope communication failure/impairments, network delay and security vulnerabilities. To overcome these issues, flexible control system, reconfigurable on the basis of the actual communication capabilities, have to be designed. In this sight, cooperative driving can be represented as a networked control system where the vehicles are controlled by handling their state information and networked information received from neighboring vehicles through the communication network [170, 167, 144] in which the time-delay and the security vulnerabilities are explicitly modeled in order to give a more realistic representation of the cooperative driving systems [151, 155, 152].

3.2 Modeling of Connected Autonomous Vehicles

Formation control of autonomous connected vehicles is one of the typical problems addressed in the context of networked multi-agent systems (e.g. for the flight formation of autonomous aerial vehicles [16]). It follows that a multi-agent system has been naturally proposed as an alternative modeling approach to easily handle the coordination of ground vehicles (cars) and to manage platoon tasks (e.g. see [162, 59, 170, 174, 167, 111, 151, 60, 92] and references therein).
By leveraging this networked control system paradigm, a platoon composed by multiple connected and automated vehicles is represented as

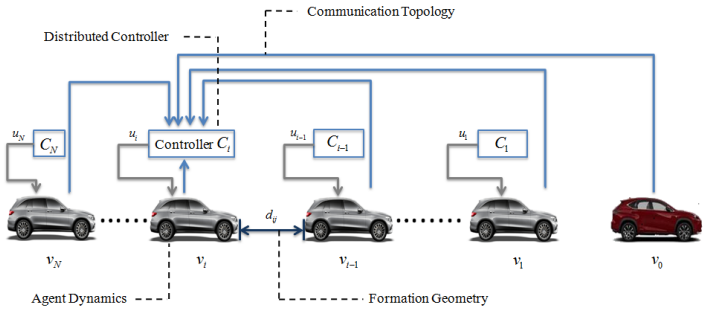


Figure 3.4: Schematic representation of autonomous connected vehicles platoons from networked control systems perspective[197].

one-dimensional network of dynamical agents, in which each agent only uses its neighboring information to locally control its motion, while it aims to achieve certain global coordination with all other agents. This framework is schematically represented in Fig. 3.4 as the composition of the following main interrelated components: *a*) agent dynamics, that model the longitudinal dynamics of each vehicle; *b*) communication topology, which indicates how and if an agent obtains information about other agents depending on the active communication links *c*) formation geometry, which defines the desired spacing between adjacent vehicles in a platoon; *d*) distributed collaborative control that is implemented at the single-vehicle level and depends on both the state variables of the vehicle itself (measured on board) and information received from neighboring vehicles through the communication topology.

3.2.1 Agent Dynamics

The behaviour of each vehicle within the vehicular network is described by its longitudinal dynamics. These latter are inherently nonlinear due to some salient nonlinearities involved in the powertrain system, e.g., engine, driveline, brake system, aerodynamics drag, tire friction, gravitational force [158].
In order to facilitate the control strategy design, the following assumption were used to obtain a concise model for cooperative driving control [116]:

1. The longitudinal tire slip is negligible;

2. The vehicle body is rigid and symmetric;

3. The influence of pitch and yaw motions are negligible;

4. The driving and braking torques are controllable inputs.

Under the aforementioned assumption, the simplified resulting longitudinal dynamics for each i-th vehicle, still nonlinear, are described as follows[170] ($\forall i = 1, \cdots, N$, being N the number of vehicle within the vehicular network):

$$\begin{aligned} &\dot{p}_i(t) = v_i(t) \\ &\tfrac{\eta_{F,i}}{r_{w,i}} F_i(t) = m_i \dot{v}_i(t) + C_{A,i} v_i^2(t) + m_i g f \\ &T_i \dot{F}_i(t) + F_i(t) = F_{des,i}(t), \end{aligned} \tag{3.1}$$

where p_i $[m]$, v_i $[m/s]$ are the position and the speed of the i-th vehicle that are measured with respect to a road reference frame; m_i, $C_{A,i}$, g, f, $\eta_{F,i}$, $r_{w,i}$ are the mass, the aerodynamics drag coefficient, the gravitational acceleration, the rolling resistance coefficient, the mechanical efficiency of driveline and the wheel radius for the i-th vehicle, respectively; $F_i(t)$ denotes the actual driving/brake force; T_i is is the characteristic time constant of the drivetrain depending upon specific features of the vehicle; $F_{des,i}(t)$ is the desired driving/brake force, i.e. the control input, that has to be imposed to vehicle dynamic in order to reach a specific control objective.
However, control performance are difficult to analytically analyze for nonlinear models [116]. To this aim, linear models are more frequently used to formulate tractable problems. The most commonly used models for describing the i-th vehicle behavior are:

1. single integrator model;

2. second-order model;

3. third-order model.

Single Integrator Model The single integrator model is the simplest model for vehicle dynamics, where the vehicle speed is taken as the control input $u_i(t)$ and the position $p_i(t)$ is the only state variable [216], i.e.

$$\dot{p}_i(t) = u_i(t). \tag{3.2}$$

Second-Order Model One improvement w.r.t. to single integrator model is to consider the vehicle dynamic as a point mass, described by the following second-order dynamics[150]:

$$\begin{aligned} \dot{p}_i(t) &= v_i(t) \\ \dot{v}_i(t) &= \tfrac{1}{m_i} u_i(t), \end{aligned} \tag{3.3}$$

where p_i $[m]$, v_i $[m/s]$ are the position and the speed of the i-th vehicle; m_i is the mass of the vehicle i; $u_i(t)$ is the control input, i.e. the desired acceleration that has to be imposed to the vehicle dynamic so to achieve the desired control objective.
Note that, although commonly exploited, the assumption of directly controlling the acceleration of the vehicle still does not capture some features of the vehicle internal dynamics, e.g. the inertial delay in powertrain dynamics, and might lead to instability in real-world driving conditions [199].

Third-Order Model The third order model is introduced so to take into account the powertrain dynamics of the vehicle. It is obtained by converting the nonlinear model (3.1) into a linear one for controller design via a feedback linearization technique [199]. Specifically, the control input $F_{des,i}(t)$ is selected as [116]

$$F_{des,i}(t) = \frac{1}{\eta_{F,i}}(C_{A,i} v_i(t)(2T_i \dot{v}_i(y) + v_t) + m_i g f + m_i u_i(t)) r_{w,i}, \tag{3.4}$$

where $u_i(t)$ is the new input after linearization. Then, the following linear model is obtained for vehicle longitudinal dynamics [131]:

$$T_i \dot{a}_i(t) + a_i(t) = u_i(t), \tag{3.5}$$

where $a_i(t)$ denotes the acceleration of vehicle i.
Considering the state space representation of model (3.5), we obtain the third order model for each vehicle as:

$$\dot{x}_i = Ax_i + Bu_i(t) \tag{3.6}$$

where $x_i(t) = [r_i(t)\ v_i(t)\ a_i(t)]^\top \in \mathbb{R}^3$ represent the i-th vehicle state vector ($i = 1, \cdots, N$) (being r_i [m] and v_i [m/s] and a_i [m/s^2] the i-th vehicle position (in meters), velocity (in meters per second) and acceleration (in meters per second^2), measured with respect to road reference frame); $A \in \mathbb{R}^{3\times3}$ and $B \in \mathbb{R}^{3\times1}$ have the following expression:

$$A = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & -\frac{1}{T_i} \end{bmatrix}, B = \begin{bmatrix} 0 \\ 0 \\ \frac{1}{T_i} \end{bmatrix}. \tag{3.7}$$

Multiple vehicle are involved in cooperative driving application, and thus an important feature for the agent dynamics is the homogeneity.

Definition 5. *A platoon of connected autonomous vehicles is said to be homogeneous if all vehicles share identical dynamics; otherwise it is called heterogeneous.*

3.2.2 Communication Topology

The communication topology in cooperative driving application indicates the way each vehicle obtains the information of its neighboring vehicles. More specifically, it describes the information used by local onboard vehicles controller and thus strongly influences the collective behavior of vehicles platoon. Early-stage cooperative driving applications were mainly based on radars and sensor to acquire information about the surrounding environment [96]. This imply that each vehicle could obtain, at most, information coming from its preceding and follower vehicles. In this case the following communication topologies arise:

- Predecessor-Follower (P-F). Each vehicle can exchange information only with its preceding vehicle;
- Bidirectional (B-F). Each vehicle can exchange information with its preceding and follower vehicles.

More recently, the development of reliable wireless vehicular communication, leveraging Vehicle-to-Vehicle (V2V) and/or Vehicle-to-Infrastructure (V2I) connectivity, has allowed the exchange of more information among vehicles and/or between a vehicle and the road infrastructure. Therefore new communication topologies, depicted in Fig. 3.5, are emerging in cooperative driving application such as [217]:

1. Leader-Predecessor-Follower (L-P-F). Each vehicle can communicate with its preceding vehicle and the leading vehicle;

2. Bidirectional-Leader-Follower (B-L-F). Each vehicle can exchange information with its preceding vehicle, its follower vehicle and the leading vehicle;

3. All-to-All (Broadcast, BR). Each vehicle exchange information with all the other vehicles in platoon.

The network communication structure can be modeled by a graph where every vehicle is a node. Hence, a network of N vehicles is represented as a directed graph (digraph) $\mathcal{G} = (\mathcal{V}, \mathcal{E}, \mathcal{A})$ of order N characterized by the set of nodes $\mathcal{V} = \{1, \ldots, N\}$ and the set of edges $\mathcal{E} \subseteq \mathcal{V} \times \mathcal{V}$. The topology of the graph is associated to an adjacency matrix with non negative elements $\mathcal{A} = [\alpha_{ij}]_{N \times N}$. In what follows, we assume $\alpha_{ij} = 1$ in the presence of a communication link from vehicle j to vehicle i, otherwise $\alpha_{ij} = 0$. Moreover, $\alpha_{ii} = 0$ (i.e., self-edges (i, i) are not allowed unless otherwise indicated). The presence of edge $(i, j) \in \mathcal{E}$ means that vehicle i can obtain information from vehicle j, but not necessarily *viceversa*. Note that, defining the degree matrix as $D = \text{diag}\{\Delta_1, \Delta_2, ..., \Delta_N\}$, with $\Delta_i = \sum_{j \in \mathcal{V}} \alpha_{ij}$, the Laplacian of the directed graph $\mathcal{G}$ can be defined as $L = D - \mathcal{A}$.

In the rest of the thesis we consider N vehicles together with a leader agent, taken as an additional agent labeled with the index zero, i.e., node 0. We use, hence, an augmented directed graph $\mathcal{G}_{N+1}$ to model the resulting network topology. We assume node 0 to be *globally reachable* in $\mathcal{G}_{N+1}$. Thus there exists a path in $\mathcal{G}_{N+1}$ from every node i in $\mathcal{G}$ to node 0 [88]. Note that, in the typical network topologies for cooperative applications, shown in Fig. 3.5, the leader is always globally reachable (see [115] and reference therein).

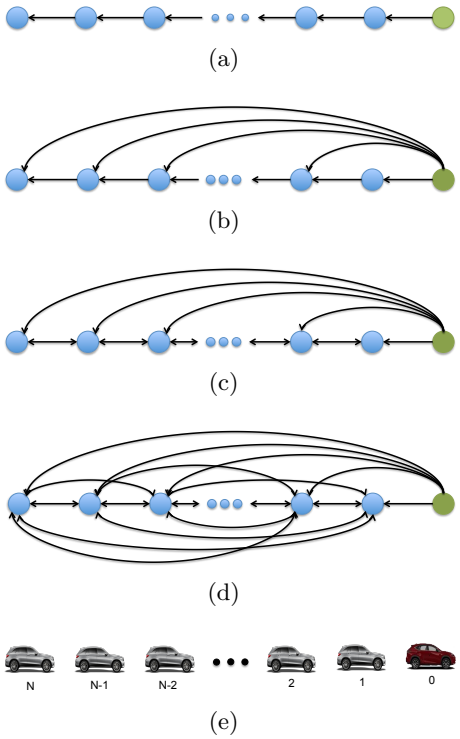


Figure 3.5: Examplar platoon communication topologies: (a) Predecessor-Following (P-F), (b): Leader-Predecessor-Following (L-P-F); (c): Bidirectional-Leader-Predecessor (B-L-F); (d): All-to-All (Broadcast, BR); (e): Platoon of $N+1$ vehicles.

3.2.3 Formation Geometry

Formation geometry defines the desired spacing between adjacent vehicles in cooperative driving application. In general, there are three main policies of formation geometry employed in cooperative driving, namely:

1. Constant distance [150, 212]. The desired distance among two adjacent vehicles is constant and independent of vehicle velocity, which can achieve a very high traffic capacity.

2. Constant Time Headway policy [170, 167, 96]. The desired inter-vehicle spacing varies with vehicle velocity, which is more likely

in accordance with driver behaviors, but has limit on achievable traffic capacity.

3. Nonlinear distance policy [98, 207, 60]. The desired inter-vehicle distance is a nonlinear function of vehicle velocity, which has the potential to balance the traffic flow stability and traffic capacity compared with constant distance and constant time headway policies (see [219] for details).

3.2.4 Distributed Controller

The distributed controllers are implemented at the single-vehicle level and depends on both the state variables of the vehicle itself (measured on board) and the information received from neighboring vehicles through the communication topology so to achieve a certain global coordination. The controller design strongly depends on the performances that the designer would achieve in cooperative driving applications. The first priority for cooperative driving application is to guarantee the internal stability, i.e. the networked closed loop system need to be asymptotically stable. In addition to the internal stability, other performances metrics include:

- String stability [176]. A vehicles platoon is string stable if the disturbances are attenuated when propagating downstream along the string of vehicle.
- Stability margin [82]. The stability margin is the real part of least stable eigenvalue that characterizes the speed of convergence to the desired behavior.
- Coherence Behavior [15]. It is quantified as the H_2 norm of the closed-loop system, capturing the robustness of the vehicle platoon w.r.t. exogenous disturbances.

The majority of distributed controller are linear for the easiness of comprehensive theoretical analysis and the convenience of hardware implementation [120]. However, there are two major drawbacks in linear design methods, namely 1) it is not easy to explicitly handle string stability, and 2) it is unable to deal with the nonlinearity and constraints. Therefore, more recently, advanced control methods have been introduced

into cooperative driving control for achieving better performances. For example, sliding mode control (SMC) [199] and H_∞ [156] controller for dealing with string stability, or Model Predictive Control (MPC) approach which explicitly handle the vehicle nonlinearities and a actuator constraints [107].
Traditionally, control algorithms are usually designed based on an implicit assumption of unlimited computation resources, non-delayed sensing and actuation, unlimited bandwidth and perfect communication environments, and control design mainly focuses on establishing the relationship between control performance and computation complexity [68]. However, computation and communication resources are limited and often shared between multiple applications (such as subsystems, agents, nodes and other processes). Thus, the development of real-time distributed control algorithms in cooperative driving applications should be realized and reevaluated by integrating communication, computation and control so as to achieve the desired control performance through local, asynchronous, distributed and cooperative actions. Therefore, another crucial performances metric that has to be considered in cooperative driving control strategy design, less addressed in the current literature, is the Resiliency and the Robustness to the unavoidable communication impairments introduced by wireless vehicular network. Moreover, vehicular networks can suffer different security threats. In view of the fact that cyber attacks can lead to dangerous implications for the security of autonomous driving systems another challenge in cooperative driving systems is the designing of distributed control protocols able to cope also with different kinds of possible cyber attacks.

3.3 Communication issues of cooperative driving application

Wireless V2V communication enables cooperative driving to exchange information among vehicles in addition to the local sensors (i.e. radar and lidar) measurements which is highly potential to improve cooperative driving performances. However, vehicular networks introduces unavoidable communication impairments such as transmission delay and packet losses [30, 218] that strongly affect the performances of cooperative driving. Communication time-delay and other networked-induced

phenomena are hence crucial in cooperative driving application since they may lead the vehicular network to instability. Therefore, for the practical implementation of distributed strategies, they have to be taken into account from the beginning of the control design phase.
Traditional control systems deal with control issues in which the data communication link between vehicles is considered to be perfect. As a result, information exchanged among vehicles is completely and exactly exploited by onboard distributed controller. This is in contrast to networked control system paradigm since in practice, when deploying distributed control strategies, agents share information through dedicated wired or wireless communication networks. Indeed, due to technological constraints, time-delays in data acquisition and transmission are unavoidable and their effects on the closed-loop network have to be investigated and prevented, since they may strongly compromise the predicted system stability, as well as the overall performance [153, 198].
The challenge in the control field is hence to design cooperative control algorithms that are resilient and robust to communication impairments. Communication time delay is defined as:

- Homogenous if the communication time delay is assumed to be equal for each communication link of the network;
- Heterogeneous if the communication time delay is different for each communication link of the network.

Moreover for each of this category, we can further assume that delays can be modeled as:

- Constant function;
- Time-varying function.

The presence of communication delays implies that the distributed control strategies have to be implemented via outdated information. It follows that the networked control system has to cooperate in the presence of time-delays that affect the control input and hence the closed-loop network. This problem has been tackled in the current literature under the restrictive assumption that the communication delay is unique (or homogeneous, uniform, identical as indifferently referred in the technical literature) and often constant (see e.g. [135, 139, 86, 90, 182, 91, 123]).

However, when treating with communication networks, e.g., based on the IEEE 802:11 protocol, each communication link, that connects a pair of agents, is affected by a different variable time-delay that depends from actual conditions, or possible impairments, of the communication channel. It follows that the hypothesis commonly made in the technical literature of a unique and constant network delay may result unrealistic and that delays, affecting the outdated information that are used to compute the control input, have to be considered as time-varying functions depending from the specific communication link under investigation, i.e. $\tau_{ij}(t)$ (multiple, or equivalently heterogeneous, time-varying delays) [153]. Indeed, time-delay itself might obey its own dynamics, which possibly depend on the communication distance, total computation load and computation capability. The thesis contributes to extend the literature on synchronization of cooperative networked systems by addressing the problem of cooperative driving in the presence of multiple time-varying communication delays.

3.4 Security issues of cooperative driving application

The Vehicular ad hoc Networks and the de facto vehicular networking standard IEEE 802.11p communication protocol are key tools for the deployment of platooning applications, since the cooperation among vehicles is based on a reliable communication structure. However, vehicular networks can suffer different security threats. Indeed, in collaborative driving applications, the sudden appearance of a malicious attack can mainly compromise: i) the correctness of data traffic flow on the vehicular network by sending malicious messages that alter the platoon formation and its coordinated motion; ii) the safety of platooning application by altering vehicular network communication capability. In view of the fact that cyber attacks can lead to dangerous implications for the security of autonomous driving systems, it is fundamental to consider their effects on the behavior of the interconnected vehicles, and to try to limit them from the control design stage. Special attention has been recently raised with respect to control solutions for cyber-physical systems in vehicular networks, where the complexity of transportation systems, and of high

mobility vehicular systems, pushes to find tailor-made solutions depending from the specific application, such as platooning (e.g. see [75, 124]). Past studies on VANETs security vulnerabilities focus their attention on an accurate classification of malicious attacks and the solutions to mitigate them at communication level [4]. However, while security in sensing and communication has been extensively investigated in the technical literature, security in control has been recently indicated as a key ingredient that has to be added for enhancing the protection level of the normal operation of a physical process.
From control viewpoint, recent literature on the security of the networked cyber-physical systems is usually devoted to designing state estimators for the better understanding of system dynamical behaviors and the attack detection (see survey [50] and references therein). Alternative approaches propose instead the exploitation of the cooperation property of the multi-agent systems paradigm, or more precisely the exploitation of all information exchanged among the agents within the networked control system [151]. However, many issues are still open, as for example the need of designing distributed control protocols for connected multi-agent systems able to cope simultaneously with network induced phenomena - such as the unavoidable delays that affect in practice the information shared via a wireless channel - and different kinds of possible cyberattacks [50]. Therefore, since security is a crucial point in cooperative driving control system design, in this thesis we also propose a distributed collaborative control strategy which is able to both counteract communication impairments, such as time-varying multiple delays, and to attenuate malicious effects on platoon behavior.

CHAPTER 4

Adaptive synchronization-based control protocol for cooperative driving of autonomous vehicles with multiple communication delays

The development of automated and coordinated driving systems is an hot topic today for vehicles and it represents a challenging scenario that heavily relies on distributed control in the presence of wireless communication network. To actuate platooning in a safe way it is necessary to design controllers able to effectively operate on informations exchanged via vehicular networks despite the presence of unavoidable communication impairments, such as multiple time-varying delays that affect communication links. To this aim in this chapter we propose a novel distributed adaptive collaborative control strategy that exploits information

coming from connected vehicles to achieve leader synchronization and we analytically demonstrate its stability with a Lyapunov-Krasovskii approach. The effectiveness of the proposed strategy is shown via numerical simulations in PLEXE, a state of the art inter-vehicle communication and mobility simulator that includes basic building blocks for platooning.

4.1 Cooperative Driving as Synchronization problem

Nowadays Intelligent Transportation Systems (ITS) lead to positive effects, in terms of pollution and safety. Connected autonomous vehicles improve the traffic flow mitigation, and a fundamental aim is to cooperatively drive the road by operating vehicle's platoon that maintain an optimal inter-vehicular spacing policy, tracking at the same time desired speed and acceleration profiles. The natural breakthrough is the improvement of road capacity and traffic congestion mitigation [37, 36], while preserving at the same time fuel economy and decrease of pollutants emissions [191, 57, 122, 126, 130].
In this driving paradigm all connected vehicles embed wireless communication hardware in order to share information with neighbors and to receive the reference signal coming from the leading vehicle. On the basis of information received from vehicles within the platoon, the onboard control algorithm is responsible of the safe tracking of the desired velocity and acceleration profile, *i.e.* vehicles have to track the leader motion while respecting at the same time a pre-determined inter-vehicles spacing policy [8, 14]. The goal is to perform a reference tracking that allows followers to pursue the leader in a safe way but guaranteeing at the same time excellent transient dynamics. Transient performance are fundamental during normal operation, when deceleration, or acceleration, maneuvers must be safely executed (*e.g.* in the occurrence of sudden traffic) avoiding that any vehicle in formation falls too far behind the vehicle ahead [158, 9]. Tracking ability assume also a great importance during join or emergency braking maneuvers, when all vehicles has to safely brake reaching their required stand-still distance when they finally stop [136, 125, 127].
Although a platoon is a group of lined vehicles, different communication

topologies arise, depending from the on board communication facilities, their features [212, 167], and how the information is used by the control algorithm. Furthermore, since vehicles are moving within a non-ideal wireless communication environment, information can be received by each vehicle with a different (multiple, or heterogeneous) time-varying delay, whose current value depends on the network conditions [30, 218]. Note that since communication impairments are unavoidable in practice, the control input, that is computed on the base of the network information, results to be affected by delay in realistic scenarios and packet losses [164].

Typical control schemes for platoon follow a Cooperative Adaptive Cruise Control (CACC) approach which adopts pre-fixed communication patterns during control design, such as, for example, predecessor-follower [158, 220]. The aim is to provide robustness to the platoon that is assumed to be already formed and traveling with a target velocity, so that small perturbation on leading vehicle are de-amplified toward the platoon tail. The analytical control synthesis is usually performed by exploiting linear tools in the frequency domain under the assumption that the inter-vehicle communication is ideal or affected by a unique constant delay. A sensitivity analysis is sometimes added to investigate the effect of delay variation. See [45], and references therein, for a recent and wide review of the technical literature.

Formation control of autonomous connected vehicles is one of the typical problems addressed in the context of networked control systems (e.g. see [162, 59, 170, 174, 167, 111, 151, 60, 92] and references therein). By leveraging this paradigm, a platoon composed by multiple connected and automated vehicles is represented as one-dimensional network of dynamical agents, in which each agent only uses its neighboring information to locally control its motion, while it aims to achieve certain global coordination with all other agents. Within this framework, the consensus-based approaches have been recently proposed in [170, 97, 167] to deal with both topology variety and heterogeneity in the time-varying communication delays, but the theoretical analysis disregards leader tracking maneuvers (when the leader dynamically changes its velocity profile) and focus on the so called leader-law [9], where the platoon first forms itself and then travels with a common constant velocity.

In particular in [97, 170] and [167] the problem of communication losses

has been theoretically investigated by exploiting stability tools for delayed networks, but neglecting acceleration profiles. An alternative approach, based on a sliding mode control, has been also recently designed in [59] in the presence of an actuation lag, but under the restrictive assumption of perfect communication among agents.

More recently, consensus has been also exploited to achieve leader-tracking by describing the drivetrain but in absence of communication delays [211]. Moreover, the reference tracking problem has been also tackled in [174] by leveraging transient synchronization for linear multi-agent systems again under the restrictive hypothesis of a perfect communication. Different control methodologies have been also proposed for leader tracking such as, for example, MPC tools in [213] where the work investigates the case of an ideal communication scenario modeled by unidirectional topologies [213]. Other approaches, alternative to MPC or consensus, solve instead leader tracking by exploiting fixed-gains control strategies that are designed again under the restrictive hypotheses of a given communication structure with a prefixed-topology and a constant and unique (homogeneous) communication delay (see [200, 150, 76] and references therein). Under these assumptions the stability analysis in the presence of certain constant amount of time delay in the leader state reception is carried out around the equilibrium solution in the Laplace domain [200, 150] or exploiting a Lyapunov approach [76].

In this chapter, instead, we proposed an adaptive distributed cooperative approach to solve the leader tracking problem, or better to synchronize the platoon to generic leader velocity profiles in the presence of communication delays, assumed to be heterogeneous (multiple) and time-varying. To perform the analytical investigation, the platoon is modeled as a multi-agent system where each vehicle is a third order dynamical agent sharing information through wireless communication links (each of them affected by a different time-varying delay). Note that synchronization among autonomous agents via local interactions is one of the benchmark problems in the recent general literature on multi-agent systems control. Here the problem is commonly tackled under the restrictive assumption of an ideal (or perfect) communication among agents [119] or supposing that the communication delay is unique (or homogeneous, uniform, identical as indifferently referred) (e.g., see [182, 123] and references therein) and often constant [146].

The proposed control strategy updates its action on the basis of state errors among the vehicle itself and the delayed state information received from neighboring vehicles through the wireless communication network. On-board controllers, that automatically compensates the outdated information caused by network delays, compute a not-identical control input since different adaptive gains are associated to each communication link. The adaptive approach provides robustness with respect to unmodeled dynamics and uncertain parameters [193, 154], so to better counteract the effects of all disturbances that always characterize real vague environments.
The platoon synchronization under the action of the adaptive strategy is analytically proved by exploiting the Lyapunov-Krasovskii method and by assuming that the leading vehicle is globally reachable, *i.e.* there exists at least a path (direct or not) that allows the information flow from leader vehicle to followers. The stability criterion is expressed as an LMI criterion that also provides the estimate of the delay margin that guarantees stability. High fidelity simulations with PLEXE [169, 170, 167] are used here to test the control strategy. PLEXE permits a deep investigation of platooning systems by coupling vehicle dynamics (e.g. mass of vehicles, engine and brakes limitations) with realistic wireless network simulation for transmission delay and beaconing strategy. Note that the communication features are intrinsically modeled within PLEXE through a realistic communications device (IEEE 802.11p card) implementation. In so doing, the control algorithm has been extensively analyzed in a realistic artificial and safe environment (before being implemented in real vehicles driving on real roads), taking into account the main possible discrepancies between the theoretical control design and its deployment (e.g. due to perturbed situations, variable conditions, information losses and communication impairments). Results for different topologies confirm the effectiveness of the approach also in case of lossy channels and under the limits imposed by realistic vehicle's dynamics. Moreover, a brief comparison with an up-to-date consensus-based protocol [170] discloses the good performance of the proposed adaptive approach in guaranteeing the leader tracking.
Summarizing, the main contribution of this chapter is twofold:

1. To design and analytically prove the effectiveness of a novel distributed adaptive approach to solve the collaborative driving prob-

lem in the presence of communication impairments such as time-varying delays.

2. To carry out a comprehensive performance evaluation analysis of the proposed strategy in order to disclose its ability in ensuring the synchronization behavior (for generic time-varying leader speed profile and for different communication network topologies) and its robustness to packet losses/hard delay (by implementing the well-known Bernoulli and Gilbert-Elliot channel models).

4.2 Cooperative Leader Tracking

Here we consider a homogeneous platoon composed by N vehicles, organized as a string (with vehicles following one another along a straight line), moving along a single lane and sharing their state information (e.g., the absolute position, the velocity, and the acceleration) with all other vehicles communicating through a V2V communication paradigm [38]. The reference trajectory is imposed by the leading vehicle (the first vehicle of platoon labelled as vehicle 0 and assumed to be globally reachable). Our target is to synchronize the dynamics of all vehicles of the platoon to the reference behavior imposed by leader. Note that the formulation of problem, described as follows, is suitable for various communication topologies, including all of those shown in Fig. 3.5. The behavior of the generic i-th vehicle in the platoon is described by the longitudinal third order dynamics in Eq. (3.6) [131], i.e.:

$$\dot{x}_i = Ax_i + Bu_i(t; \tau_{ij}(t)) \tag{4.1}$$

where $x_i(t) = [r_i(t)\ v_i(t)\ a_i(t)]^\top \in \mathbb{R}^3$ represent the i-th vehicle state vector ($i = 1, \cdots, N$) (being r_i [m] and v_i [m/s] and a_i [m/s^2] the i-th agent position (in meters), velocity (in meters per second) and acceleration (in meters per second^2), measured with respect to road reference frame); $A \in \mathbb{R}^{3\times3}$ and $B \in \mathbb{R}^{3\times1}$ have the following expression:

$$A = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & -\frac{1}{T} \end{bmatrix}, B = \begin{bmatrix} 0 \\ 0 \\ \frac{1}{T} \end{bmatrix}; \tag{4.2}$$

being $T > 0$ [s] the characteristic time constant of the drivetrain depending upon specific features; $u_i(t; \tau_{ij}(t))$ the control input evaluated from each agent by exploiting both local measurements and networks information affected by time-varying delays depending on the specific communication link, i.e. $\tau_{ij}(t)$ $(j = 0, \cdots, N)$ $i \neq j$. The reference leading dynamics are instead described as [87]:

$$\dot{x}_0(t) = Ax_0(t) \tag{4.3}$$

with $x_0(t) = [r_0(t)\ v_0(t)\ a_0(t)]^\top \in \mathbb{R}^3$ and $A \in \mathbb{R}^{3\times 3}$.
The cooperative leader tracking problem, maintaining a desired inter-vehicle spacing policy, can now be expressed as the following third-order network synchronization problem:

$$\begin{array}{ll} \lim_{t\to\infty} \|r_i(t) - r_0(t) - d_{i0}\| = 0 & \\ \lim_{t\to\infty} \|v_i(t) - v_0(t)\| = 0 & \forall i = 1, ..., N, \\ \lim_{t\to\infty} \|a_i(t) - a_0(t)\| = 0 & \end{array} \tag{4.4}$$

being d_{i0} the desired distance of vehicle i from the leading vehicle [212, 186].
To solve the problem we use the following distributed strategy that leverages on an adaptive proportional controller that updates its action based on the errors among the state information as:

$$u_i = -\sum_{j=0}^{N} \alpha_{ij} k_{ij}^\top(t) \begin{bmatrix} r_i(t - \tau_{ij}(t)) - r_j(t - \tau_{ij}(t)) - d_{ij} \\ v_i(t - \tau_{ij}(t)) - v_j(t - \tau_{ij}(t)) \\ a_i(t - \tau_{ij}(t)) - a_j(t - \tau_{ij}(t)) \end{bmatrix} \tag{4.5}$$

where α_{ij} models the network topology emerging from the presence/absence of a communication link between the i-th and j-th vehicle; d_{ij} are the desired spacing errors between vehicles i and j ($\forall i = 1, \cdots, N$ and $j = 0, \cdots, N$), defined according to the spacing policy [150, 212]; $\kappa_{ij}(t) \in \mathbb{R}^{3\times 1}$ are the adaptive control gains vector. Since vehicles share information through a wireless communication channel (V2V communication paradigm), it happens that information can be delivered with time-delay. In particular a frame can be lost due to interferences, and the receiver has to wait another beacon interval before receiving the next update. The above considerations leads to the need of running the controller based on outdated information and of using the time stamp

inserted into messages to correctly correlate the information, and hence to correctly compensate the error. Indeed $\tau_{ij}(t)$ is detectable [32, 170]. The gains vector in (4.5) is given as:

$$k_{ij}(t) = \begin{bmatrix} \rho_{ij}(t) \\ \beta_{ij}(t) \\ \gamma_{ij}(t) \end{bmatrix}; \tag{4.6}$$

being $i \neq j$, and the gain vector components are updated according to the following adaption law:

$$\begin{cases} \dot{\rho}_{ij}(t) & = \zeta_{ij,1} \left(r_i(t) - r_j(t) - d_{ij} \right)^2 \\ \dot{\beta}_{ij}(t) & = \zeta_{ij,2} \left(v_i(t) - v_j(t) \right)^2 \\ \dot{\gamma}_{ij}(t) & = \zeta_{ij,3} \left(a_i(t) - a_j(t) \right)^2 \end{cases} \tag{4.7}$$

where $\zeta_{ij,k} \in \mathbb{R}^+$ $(\forall k = 1, 2, 3)$ are positive constants. Note that the initial conditions are arbitrarily set to positive values, i.e. $k_{ij}(0) > 0$.

4.2.1 Closed-Loop Vehicular Network

To prove the cooperative synchronization of vehicles dynamics (4.1) to the leader motion (4.3) under the action of the adaptive protocol in (4.5), we define the error of the i-th and the j-th vehicle with respect to leader as:

$$e_i(t) = \begin{bmatrix} r_i(t) - r_0(t) - d_{i0} \\ v_i(t) - v_0(t) \\ a_i(t) - a_0(t) \end{bmatrix} = \begin{bmatrix} \widetilde{r}_i \\ \widetilde{v}_i \\ \widetilde{a}_i \end{bmatrix} \tag{4.8}$$

$$e_j(t) = \begin{bmatrix} r_j(t) - r_0(t) - d_{j0} \\ v_j(t) - v_0(t) \\ a_j(t) - a_0(t) \end{bmatrix} = \begin{bmatrix} \widetilde{r}_j \\ \widetilde{v}_j \\ \widetilde{a}_j \end{bmatrix}. \tag{4.9}$$

After some algebraic manipulations the control strategy u_i in (4.5) can be expressed in terms of the state errors as:

$$u_i = -\sum_{j=0}^{N} \alpha_{ij} k_{ij}^{\top}(t) \left[e_i(t - \tau_{ij}(t)) - e_j(t - \tau_{ij}(t)) \right]. \tag{4.10}$$

Now the dynamics of the error system for the generic i-th vehicle under the control action (4.10) can be written as:

$$\begin{aligned}
&\dot{\widetilde{r}}_i(t) = \widetilde{v}_i(t)\\
&\dot{\widetilde{v}}_i(t) = \widetilde{a}_i(t)\\
&\dot{\widetilde{a}}_i(t) = -\tfrac{1}{T}\widetilde{a}_i(t) - \tfrac{1}{T}\sum_{j=0}^{N}\alpha_{ij}k_{ij}^{\top}(t)\left[e_i(t-\tau_{ij}(t)) - e_j(t-\tau_{ij}(t))\right].
\end{aligned} \tag{4.11}$$

System (4.11) can be recast in a more compact form as:

$$\begin{aligned}
\dot{e}_i(t) = \;& Ae_i(t) - B\alpha_{i0}k_{i0}^{\top}(t)e_i(t-\tau_{i0}(t))\\
&-B\sum_{j=1}^{N}\alpha_{ij}k_{ij}^{\top}(t)\left[e_i(t-\tau_{ij}(t)) - e_j(t-\tau_{ij}(t))\right]
\end{aligned} \tag{4.12}$$

where A and B are in (4.2).
Now, by defining

$$-B\alpha_{i0}k_{i0}^{\top}(t) = \mathcal{C}_{i0}(t) \in \mathbb{R}^{3\times 3}, \tag{4.13a}$$

$$-B\alpha_{ij}k_{ij}^{\top}(t) = \widehat{\mathcal{C}}_{ij}(t) \in \mathbb{R}^{3\times 3}, \tag{4.13b}$$

system (4.12) can be rewritten as ($i = 1, \ldots, N$):

$$\begin{aligned}
\dot{e}_i(t) = \;& Ae_i(t) + \mathcal{C}_{i0}(t)e_i(t-\tau_{i0}(t)) +\\
&\sum_{j=1}^{N}\widehat{\mathcal{C}}_{ij}(t)\left[e_i(t-\tau_{ij}(t)) - e_j(t-\tau_{ij}(t))\right].
\end{aligned} \tag{4.14}$$

Exploiting a more compact notation, delays $\tau_{ij}(t)$ can be represented as elements of the following delay set: $\sigma_p(t) \in \{\tau_{ij}(t) : i, j = 1, 2, ..., N, i \neq j)\}$ for $p = 1, 2, ..., m$ with $m \leq N(N-1)$. Analogously, delays $\tau_{i0}(t)$ are elements of the set: $\tau_l(t) \in \{\tau_{i0}(t) : i = 1, 2, ..., N, \}$ for $l = 1, 2, ..., q$ with $q \leq N$. Note that m and q are equal to their maximum value if the underlying network topology is a directed complete graph and all time-delays are different.
By defining now the error state vector as $\widetilde{x}(t) = \left[\, e_1^{\top}(t)\; e_2^{\top}(t)\; \cdots\; e_N^{\top}(t) \,\right]^{\top} \in \mathbb{R}^{3N}$, according to the above definitions, the multi-agent delayed closed-loop network can be written as:

$$\dot{\widetilde{x}}(t) = A_0\widetilde{x}(t) + \sum_{l=1}^{q}C_l(t)\widetilde{x}(t-\tau_l(t)) + \sum_{p=1}^{m}\widehat{\mathcal{C}}_p(t)\widetilde{x}(t-\sigma_p(t)) \tag{4.15}$$

where

$$A_0 = \begin{bmatrix} A & 0^{3\times3} & \cdots & 0^{3\times3} \\ 0^{3\times3} & A & \cdots & \vdots \\ \vdots & \vdots & \ddots & \vdots \\ 0^{3\times3} & \cdots & \cdots & A \end{bmatrix} \in \mathbb{R}^{3N\times3N}; \tag{4.16}$$

$$C_l(t) = \begin{bmatrix} \mathcal{C}_{(1,1)}(t) & 0^{3\times3} & \cdots & 0^{3\times3} \\ 0^{3\times3} & \mathcal{C}_{(2,2)}(t) & \cdots & \vdots \\ \vdots & \vdots & \ddots & \vdots \\ 0^{3\times3} & \cdots & \cdots & \mathcal{C}_{(N,N)}(t) \end{bmatrix} \in \mathbb{R}^{3N\times3N}, \tag{4.17}$$

with diagonal blocks such that $(i = 1, \ldots, N\ ; l = 1, \ldots, q)$

$$\mathcal{C}^{3\times3}_{(i,i)}(t) = \begin{cases} \mathcal{C}_{i0}(t) & i = l, \tau_l(\cdot) = \tau_{il}(\cdot), \\ 0^{3\times3} & i \neq l, \tau_l(\cdot) \neq \tau_{il}(\cdot), \end{cases} \tag{4.18}$$

being $\mathcal{C}_{i0}(t)$ as in (4.13a). Matrices $\widehat{\mathcal{C}}_p(t) \in \mathbb{R}^{3N\times3N}$ $(p = 1, \cdots, m)$ in (4.15) are instead block matrices such that each block (referred for the sake of clarity as $\widehat{\mathcal{C}}_{p(r,q)}(t) \in \mathbb{R}^{3\times3}$) is given as:

$$\widehat{\mathcal{C}}_{p(r,q)}(t) = \begin{cases} \widehat{\mathcal{C}}_{ij}(t) & \text{with } i \neq j \quad \text{if} \quad \sigma_p(\cdot) = \tau_{ij}(\cdot)\ , r = q = i \\ -\widehat{\mathcal{C}}_{ij}(t) & \text{with } i \neq j \quad \text{if} \quad \sigma_p(\cdot) = \tau_{ij}(\cdot)\ , r = i, q = j \\ 0^{3\times3} & \text{otherwise} \end{cases} \tag{4.19}$$

being $r, q = \{1, 2, \cdots N\}$ and $\widehat{\mathcal{C}}_{ij}(t)$ as in in (4.13b).

Given the above definitions, it holds:

Lemma 4. *Let matrices A_0, $C_l(t)$ and $\widehat{\mathcal{C}}_p(t)$ to be defined as in (4.16), (4.17) and in (4.19), respectively. Assume that node 0 is globally reachable in $\mathcal{G}_{N+1}$, then*

$$F(t) = A_0 + \sum_{l=1}^{q} C_l(t) + \sum_{p=1}^{m} \widehat{\mathcal{C}}_p(t) \in \mathbb{R}^{3N\times3N} \tag{4.20}$$

is a negative definite matrix $\forall t \geq 0$.

Proof. By construction $F(t)$ is a strictly diagonally dominant block matrix [58], whose generic block element $F_{(i,i)}(t) \in \mathbb{R}^{3\times 3}$ on the main diagonal is defined as:

$$F_{(i,i)}(t) = A + \mathcal{C}_{i0}(t) + \sum_{j=1,\, j\neq i}^{N} \widehat{\mathcal{C}}_{ij}(t) \tag{4.21}$$

with A, $\mathcal{C}_{i0}(t)$ and $\widehat{\mathcal{C}}_{ij}(t)$ as in (4.2), (4.13a) and (4.13b) respectively. Hence, to show that $F(t)$ is negative definite, it suffices to prove that each block $F_{(i,i)}(t)$ is a negative definite matrix ($i = 1, \ldots, N$).
By construction $\dot{k}_{ij}(t) \geq 0$, being $k_{ij}(0) > 0$ (see (4.7)). Then, according to (4.13b), the term $\sum_{j=1,\, j\neq i}^{N} \widehat{\mathcal{C}}_{ij}(t)$ is negative semidefinite. Now to show that blocks $F_{(i,i)}(t)$ are negative definite we have only to prove that matrices $A + \mathcal{C}_{i0}(t)$ are negative definite for $i = 1, \ldots, N$. Given the definitions in (4.2) and in (4.13a), under the assumption that node 0 is globally reachable in $\mathcal{G}_{N+1}$ we have:

$$A + \mathcal{C}_{i0}(t) = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ -\frac{1}{T}\rho_{i0}(t) & -\frac{1}{T}\beta_{i0}(t) & -\frac{1}{T}\left(1 + \gamma_{i0}(t)\right) \end{bmatrix} \tag{4.22}$$

and in so doing the statement is proven. □

4.3 Stability Analysis

Before providing stability conditions, we introduce a model transformation based on the Leibniz-Newton formula (see Definition 4) [72], i.e.:

$$\widetilde{x}(t - \tau(t)) = \widetilde{x}(t) - \textstyle\int_{t-\tau(t)}^{t} \dot{\widetilde{x}}(s)ds \ , \tag{4.23}$$

and, hence, we recast system (4.12) as:

$$\begin{aligned} \dot{\widetilde{x}}\,(t) = \ & A_0\widetilde{x}\,(t) + \sum_{l=1}^{q} C_l(t)\widetilde{x}\,(t) - \sum_{l=1}^{q} C_l(t) \textstyle\int_{t-\tau_l(t)}^{t} \dot{\widetilde{x}}(s)ds \\ & + \sum_{p=1}^{m} \widehat{\mathcal{C}}_p(t)\widetilde{x}\,(t) - \sum_{p=1}^{m} \widehat{\mathcal{C}}_p(t) \textstyle\int_{t-\sigma_p(t)}^{t} \dot{\widetilde{x}}(s)ds. \end{aligned} \tag{4.24}$$

Now, taking into account the definition of matrix $F(t)$ as in (4.20), we have:

$$\dot{\widetilde{x}}\,(t) = F(t)\widetilde{x}\,(t) - \sum_{l=1}^{q} C_l(t) \int_{t-\tau_l(t)}^{t} \dot{\widetilde{x}}(s)ds - \sum_{p=1}^{m} \widehat{\mathcal{C}}_p(t) \int_{t-\sigma_p(t)}^{t} \dot{\widetilde{x}}(s)ds\ . \tag{4.25}$$

Given the closed-loop delayed system in (4.25) the cooperative leader tracking in the presence of multiple (or heterogeneous) time-varying V2V delays is proved here under the common assumption that delays are bounded [72, 63], i.e. $\sigma_p(t) \in [0, \sigma_p^\star]$, $\dot{\sigma_p}(t) \in (0, d_p]$ $\forall t$, $\forall p$ and $d_p \leq 1$ and $\tau_l(t) \in [0, \tau_l^\star]$, $\dot{\tau_l}(t) \in (0, d_l]$ $\forall t$, $\forall l$ and $d_l \leq 1$.
The stability criterion, used to ensure leader synchronization, is expressed as an LMI criterion that allows to compute the maximum admissible delays margin by exploiting a Lyapunov-Krasovskii approach according to the following Theorem.

Theorem 5. *Consider the closed loop system under the action of the adaptive control law (4.5) as in (4.25). Assume delays $\sigma_p(t)$ $(p = 1, ..., m)$ and $\tau_l(t)$ $(l = 1, ..., q)$ to be bounded and node 0 to be globally reachable in $\mathcal{G}_{N+1}$. Given an upper bound of time-delay functions $\tau^\star = \max_{l,p}\{\tau_l^\star, \sigma_p^\star\} > 0$, if there exist the following positive-definite matrices $P, Q_l, Q_p, R \in \mathbb{R}^{3N\times 3N}$ and a positive scalar η such that the following LMIs hold:*

$$\eta\frac{q\tau^\star}{2}R - Q_l(1-d_l) < 0, \tag{4.26a}$$

$$\eta\frac{m\tau^\star}{2}R - Q_p(1-d_p) < 0, \tag{4.26b}$$

$$F^\top(t)P + PF(t) + (q+m)\tau^\star\mathcal{M}(t) + \frac{1}{\eta}\sum_{l=1}^{q} Q_l + \frac{1}{\eta}\sum_{p=1}^{m} Q_p < 0 \tag{4.26c}$$

being

$$\mathcal{M}(t) = \left[\sum_{l=1}^{q} PC_l(t)R^{-1}C_l^\top(t)P + \sum_{p=1}^{m} P\widehat{\mathcal{C}}_p(t)R^{-1}\widehat{\mathcal{C}}_p^\top(t)P + R\right], \tag{4.27}$$

then the cooperative delayed vehicular network achieves leader synchronization, i.e.

$$\lim_{t\to\infty} \widetilde{x}(t) = 0; \tag{4.28}$$

and the adaptive gains converge to a constant value vector, say $k_{ij}^{\star} \in \mathbb{R}^3$, *as*

$$\lim_{t\to\infty} k_{ij}(t) = k_{ij}^{\star}. \tag{4.29}$$

Proof. To prove the stability, we consider the following Krasovskii functional:

$$V(\widetilde{x}(t)) = V_1(\widetilde{x}(t)) + V_2(\widetilde{x}(t)) + V_3(\widetilde{x}(t)) + V_4(\widetilde{x}(t), \kappa_{ij}(t)) \tag{4.30}$$

being

$$V_1(\widetilde{x}(t)) = \eta \widetilde{x}^{\top}(t) P \widetilde{x}(t) \tag{4.31a}$$

$$V_2(\widetilde{x}(t)) = \sum_{l=1}^{q} \int_{t-\tau_l(t)}^{t} \widetilde{x}^{\top}(s) Q_l \widetilde{x}(s) ds \tag{4.31b}$$

$$V_3(\widetilde{x}(t)) = \sum_{p=1}^{m} \int_{t-\sigma_p(t)}^{t} \widetilde{x}^{\top}(s) Q_p \widetilde{x}(s) ds \tag{4.31c}$$

$$V_4(\widetilde{x}(t), \kappa_{ij}(t)) = \sum_{i=1}^{N} \sum_{j=0}^{N} \frac{1}{2} \left[k_{ij}^{\star} - k_{ij}(t)\right]^{\top} \left[k_{ij}^{\star} - k_{ij}(t)\right] \tag{4.31d}$$

where Q_l, Q_p and $P \in \mathbb{R}^{3N\times 3N}$ are constant symmetric and positive defined matrices to be determined and η is a positive scalar.
Furthermore, according to the Lyapunov-Krasovskii approach in Theorem 4, we define the following positive continuous non-decreasing functions:

$$\alpha(\widetilde{x}(t)) = \widetilde{x}^{\top}(t) P \widetilde{x}(t) \tag{4.32}$$

and

$$\begin{aligned} \beta(\widetilde{x}(t-\tau^{\star})) = \; & \eta \widetilde{x}^{\top}(t) P \widetilde{x}(t) + \sum_{l=1}^{q} \textstyle\int_{t-\tau^{\star}}^{t} \widetilde{x}^{\top}(s) Q_l \widetilde{x}(s) ds + \\ & \sum_{p=1}^{m} \textstyle\int_{t-\tau^{\star}}^{t} \widetilde{x}^{\top}(s) Q_p \widetilde{x}(s) ds \\ & + \sum_{i=1}^{N} \sum_{j=0}^{N} \tfrac{1}{2} (k_{ij}^{\star} - k_{ij}(t))^{\top} (k_{ij}^{\star} - k_{ij}(t)) \end{aligned} \tag{4.33}$$

where $\tau^{\star} = \max_{l,p}\{\tau_l^{\star}, \sigma_p^{\star}\}$ is such that:

$$\alpha(\widetilde{x}(t)) \leq V(\widetilde{x}(t)) \leq \beta(\widetilde{x}(t-\tau^{\star})). \tag{4.34}$$

Now, differentiating $V_1(\widetilde{x}(t))$ in Eq. (4.31a) along the trajectories of the system in (4.25), we have:

$$\begin{aligned}\dot{V}_1(\widetilde{x}(t)) = \; & \eta\widetilde{x}^\top(t)\left(F^\top(t)P + PF(t)\right)\widetilde{x}(t) \\ & -2\eta\widetilde{x}^\top(t)P\sum_{l=1}^{q} C_l(t)\int_{t-\tau_l(t)}^{t}\dot{\widetilde{x}}(s)ds \\ & -2\eta\widetilde{x}^\top(t)P\sum_{p=1}^{m}\widehat{\mathcal{C}}_p(t)\int_{t-\sigma_p(t)}^{t}\dot{\widetilde{x}}(s)ds.\end{aligned} \tag{4.35}$$

According to Lemma 3, for any matrix positive definite R it holds

$$\begin{aligned}-2x^\top(t)PC\int_{t-h}^{t}x(s)ds \leq \; & \bar{h}x^\top(t)PCR^{-1}C^\top Px(t) \\ & +\int_{t-h}^{t}x^\top(s)Rx(s)ds\end{aligned} \tag{4.36}$$

being $\bar{h}$ maximum value assumed by a time delay. Under the assumption of delays boundedness [63], inequality (4.36) can be applied to (4.35), thus yielding:

$$\begin{aligned}\dot{V}_1(\widetilde{x}(t)) \leq \; & \eta\widetilde{x}^\top(t)\left(F^\top(t)P + PF(t)\right)\widetilde{x}(t) \\ & +\eta\sum_{l=1}^{q}\tau_l^\star\widetilde{x}^\top(t)PC_l(t)R^{-1}C_l^\top(t)P\widetilde{x}(t) \\ & +\eta\int_{t-\tau_l(t)}^{t}\dot{\widetilde{x}}^\top(s)R\dot{\widetilde{x}}(s)ds \\ & +\eta\sum_{p=1}^{m}\sigma_p^\star\widetilde{x}^\top(t)P\widehat{\mathcal{C}}_p(t)R^{-1}\widehat{\mathcal{C}}_p^\top(t)P\widetilde{x}(t) \\ & +\eta\int_{t-\tau_l(t)}^{t}\dot{\widetilde{x}}^\top(s)R\dot{\widetilde{x}}(s)ds.\end{aligned} \tag{4.37}$$

Applying now the Jensen inequality for the integral terms (see Lemma 2), inequality (4.37) can be easily re-written after some algebraic manipulations as:

$$\begin{aligned}\dot{V}_1(\widetilde{x}(t)) \leq \; & \eta\widetilde{x}^\top(t)\left(F^\top(t)P + PF(t) + \sum_{l=1}^{q}\tau_l^\star PC_l(t)R^{-1}C_l^\top(t)P + \right. \\ & \left.\sum_{p=1}^{m}\sigma_p^\star P\widehat{\mathcal{C}}_p(t)R^{-1}\widehat{\mathcal{C}}_p^\top(t)P + \sum_{l=1}^{q}\frac{\tau_l^\star}{2}R + \sum_{p=1}^{m}\frac{\sigma_p^\star}{2}R\right)\widetilde{x}(t) + \\ & \eta\sum_{l=1}^{q}\frac{\tau_l^\star}{2}\left(\widetilde{x}^\top(t-\tau_l(t))R\widetilde{x}^\top(t-\tau_l(t))\right) \\ & +\eta\sum_{p=1}^{m}\frac{\sigma_p^\star}{2}\left(\widetilde{x}^\top(t-\sigma_p(t))R\widetilde{x}^\top(t-\sigma_p(t))\right).\end{aligned} \tag{4.38}$$

Consider now the maximum delay bound for all the different time-delay functions associated to the each single link, i.e. $\tau^\star = \max_{l,p}\{\tau_l^\star, \sigma_p^\star\}$. Since $\sum_{l=1}^{q} \tau_l^\star \leq q\tau^\star$ and $\sum_{p=1}^{m} \sigma_p^\star \leq m\tau^\star$, inequality (4.38) can be finally be recast in a more compact form as:

$$\begin{aligned}\dot{V}_1(\widetilde{x}(t)) \leq \quad & \eta\widetilde{x}^\top(t)\left(F^\top(t)P + PF(t) + (q+m)\tau^\star\mathcal{M}(t)\right)\widetilde{x}(t) \\ & +\eta\tfrac{q\tau^\star}{2}\sum_{l=1}^{q}\left(\widetilde{x}^\top(t-\tau_l(t))R\widetilde{x}^\top(t-\tau_l(t))\right) \\ & +\eta\tfrac{m\tau^\star}{2}\sum_{p=1}^{m}\left(\widetilde{x}^\top(t-\sigma_p(t))R\widetilde{x}^\top(t-\sigma_p(t))\right).\end{aligned} \tag{4.39}$$

being

$$\mathcal{M}(t) = \sum_{l=1}^{q} PC_l(t)R^{-1}C_l^\top(t)P + \sum_{p=1}^{m} P\widehat{\mathcal{C}}_p(t)R^{-1}\widehat{\mathcal{C}}_p^\top(t)P + R. \tag{4.40}$$

From (4.31b), by differentiating $V_2(\widetilde{x}(t))$ along the trajectories of the system in (4.25), we have:

$$\dot{V}_2(\widetilde{x}(t)) = \sum_{l=1}^{q}\widetilde{x}^\top(t)Q_l\widetilde{x}(t) - \sum_{l=1}^{q}\widetilde{x}^\top(t-\tau_l(t))Q_l\widetilde{x}(t-\tau_l(t))\left(1-\dot{\tau}_l(t)\right), \tag{4.41}$$

and then, assuming that all delays are bounded, it holds:

$$\dot{V}_2(\widetilde{x}(t)) \leq \sum_{l=1}^{q}\widetilde{x}^\top(t)Q_l\widetilde{x}(t) - \sum_{l=1}^{q}\widetilde{x}^\top(t-\tau_l(t))Q_l\left(1-d_l\right)\widetilde{x}(t-\tau_l(t)). \tag{4.42}$$

Analogously, following the above steps in the case of $V_3(\widetilde{x}(t))$ in (4.31c) we get

$$\dot{V}_3(\widetilde{x}(t)) \leq \sum_{p=1}^{m}\widetilde{x}^\top(t)Q_p\widetilde{x}(t) - \sum_{p=1}^{m}\widetilde{x}^\top(t-\sigma_p(t))Q_p\left(1-d_p\right)\widetilde{x}(t-\sigma_p(t)), \tag{4.43}$$

while differentiating $V_4(\kappa_{ij}(t))$ in (4.31d) along the trajectories of the system it holds

$$\dot{V}_4(k_{ij}(t)) = -\sum_{i=1}^{N}\sum_{j=0}^{N}\left[k_{ij}^\star - k_{ij}(t)\right]^\top\dot{k}_{ij}(t). \tag{4.44}$$

By summing (4.39),(4.42),(4.43) and (4.44), after some algebraic manipulations we have:

$$\begin{aligned}\dot{V}(\cdot) \leq \quad & \eta\widetilde{x}^{\top}(t)\left(F^{\top}(t)P + PF(t) + (q+m)\tau^{\star}\mathcal{M}(t)\right. \\ & \left. +\tfrac{1}{\eta}\textstyle\sum_{l=1}^{q} Q_l + \tfrac{1}{\eta}\sum_{p=1}^{m} Q_p\right)\widetilde{x}(t) \\ & + \sum_{l=1}^{q}\widetilde{x}^{\top}(t-\tau_l(t))\left(\eta\tfrac{q\tau^{\star}}{2}R - Q_l\left(1-d_l\right)\right)\widetilde{x}^{\top}(t-\tau_l(t)) \\ & + \sum_{p=1}^{m}\widetilde{x}^{\top}(t-\sigma_p(t))\left(\eta\tfrac{m\tau^{\star}}{2}R - Q_p\left(1-d_p\right)\right)\widetilde{x}^{\top}(t-\sigma_p(t)) \\ & - \sum_{i=1}^{N}\sum_{j=0}^{N}\left[k_{ij}^{\star} - k_{ij}(t)\right]^{\top}\dot{k}_{ij}(t).\end{aligned} \tag{4.45}$$

Define now the following augmented state vector

$$\xi(t) = [\widetilde{x}(t-\tau_1(t)), \cdots, \widetilde{x}(t-\tau_q(t)), \widetilde{x}(t-\sigma_1(t)), \cdots, \widetilde{x}(t-\sigma_m(t))]^{\top} \tag{4.46}$$

and denote

$$H(t) = F^{\top}(t)P + PF(t) + (q+m)\tau^{\star}\mathcal{M}(t) + \tfrac{1}{\eta}\sum_{l=1}^{q} Q_l + \tfrac{1}{\eta}\sum_{p=1}^{m} Q_p. \tag{4.47}$$

Inequality (4.45) can be now rewritten in a more compact form as:

$$\begin{aligned}\dot{V}(\widetilde{x}(t), k_{ij}(t)) \leq \quad & \eta\widetilde{x}^{\top}(t)H(t)\widetilde{x}(t) + \xi^{\top}(t)\Theta\xi(t) \\ & - \sum_{i=1}^{N}\sum_{j=0}^{N}\left[k_{ij}^{\star} - k_{ij}(t)\right]^{\top}\dot{k}_{ij}(t)\end{aligned} \tag{4.48}$$

where $\Theta \in \mathbb{R}^{\upsilon\times\upsilon}$ ($\upsilon = 3N(q+m)$) is the following diagonal block matrix:

$$\Theta = \begin{bmatrix} \theta_{1,1} & 0^{3N\times 3N} & \dots & \dots & \dots & \dots & 0^{3N\times 3N} \\ 0^{3N\times 3N} & \theta_{2,2} & 0^{3N\times 3N} & \dots & \dots & \dots & \vdots \\ \vdots & \ddots & \ddots & \ddots & \dots & \dots & \vdots \\ \vdots & \ddots & 0^{3N\times 3N} & \theta_{q,q} & 0^{3N\times 3N} & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & \theta_{q+1,q+1} & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & \ddots & \ddots & 0^{3N\times 3N} \\ 0^{3N\times 3N} & \dots & \dots & \dots & \dots & 0^{3N\times 3N} & \theta_{q+m,q+m} \end{bmatrix} \tag{4.49}$$

whose diagonal blocks are given as follows:

$$\theta_{h,h}^{3N\times 3N} = \begin{cases} \eta\frac{q\tau^\star}{2}R - Q_l(1-d_l) & \text{for } h = l = 1,\dots,q; \\ \eta\frac{m\tau^\star}{2}R - Q_p(1-d_p) & \text{for } h = q+p,\ p = 1,\dots,m. \end{cases} \tag{4.50}$$

Inequality (4.48) can be finally recast as:

$$\dot{V}(\widetilde{x}(t)) \leq \Phi_1(\xi(t)) + \Phi_2(\widetilde{x}(t), k_{ij}(t)) + \Phi_3(\widetilde{x}(t), k_{ij}(t)), \tag{4.51}$$

being

$$\Phi_1(\xi(t)) = \xi^\top(t)\Theta\xi(t); \tag{4.52a}$$

$$\Phi_2(\widetilde{x}(t), k_{ij}(t)) = \eta\widetilde{x}^\top(t)H(t)\widetilde{x}(t); \tag{4.52b}$$

$$\Phi_3(\widetilde{x}(t), k_{ij}(t)) = -\sum_{i=1}^{N}\sum_{j=0}^{N}(k_{ij}^\star - k_{ij}(t))^\top(\dot{k}_{ij}(t)). \tag{4.52c}$$

Hence, if (4.26a), (4.26b) and (4.26c) are satisfied, then $\Phi_1(\xi(t))$ in (4.52a) and $\Phi_2(\widetilde{x}(t), k_{ij}(t))$ in (4.52b) are negative definite. Therefore from (4.51), to have $\dot{V}(t) < 0$ it suffices to show that $\Phi_3(\widetilde{x}(t), k_{ij}(t))$ is non positive. Obviously, if each $k_{ij}(t)$ is upper bounded, given that by construction $\dot{k}_{ij}(t) \geq 0$ then there exists a value of each arbitrary vector $k_{ij}^\star$ that guarantees asymptotic stability of the system (4.25).
Otherwise, in what follows we show that if $k_{ij}(t)$ were unbounded, we

would get a contradiction. Both $\Phi_2(\widetilde{x}(t), k_{ij}(t))$ and $\Phi_3(\widetilde{x}(t), k_{ij}(t))$ are quadratic function of the synchronization errors $\widetilde{x}(t)$. Moreover, $\Phi_2(\widetilde{x}(t), k_{ij}(t))$ is a quadratic function of the various $k_{ij}(t)$ while $\Phi_3(\widetilde{x}(t), k_{ij}(t))$ is a linear function of these various gains. Hence, if $k_{ij}(t)$ diverged, both $\Phi_2(\widetilde{x}(t), k_{ij}(t))$ and $\Phi_3(\widetilde{x}(t), k_{ij}(t))$ would also diverge. Thus, it is possible to find a suitable value of the constant η in (4.52b) so that $|\Phi_2(\widetilde{x}(t), k_{ij}(t))| \geq |\Phi_3(\widetilde{x}(t), k_{ij}(t))| \; \forall \; \widetilde{x}(t)$ and $k_{ij}(t)$. Since $\Phi_2(\widetilde{x}(t), k_{ij}(t))$ is negative definite from the hypothesis, we have that $\dot{V}(t) < 0 \; \forall \; \widetilde{x}(t)$ and $k_{ij}(t)$ against the assumption that $k_{ij}(t)$ diverged. Hence $k_{ij}(t)$ are upper bounded and being $k_{ij}(t)$ monotone increasing, it follows $\lim_{t\to\infty} k_{ij}(t) = c_{ij} < +\infty$. Choosing $c_{ij} = k_{ij}^{\star}$, we have that $\dot{V}(t) < 0$ and thus condition (2.23) of Theorem 4 is satisfied. In addiction, choosing $\alpha(s)$ as in (4.32), it follows that $\lim_{s\to\infty} \alpha(s) = +\infty$, and hence system (4.25) is globally uniformly asymptotically stable and synchronization is proved.
Finally, since $k_{ij}(t)$ are upper bounded, we can compute the matrices defined in (4.20) and (4.40) for $k_{ij}(t) = k_{ij}^{\star}$ and we indicate them as $F^{\star}$ and $C^{\star}$, respectively. Then the delay margin can be estimated from (4.26c) as

$$\tau^{\star} = \frac{\|F^{\star\top}P + PF^{\star} + \frac{1}{\eta}\left(\sum_{l=1}^{q} Q_l + \sum_{p=1}^{m} Q_p\right)\|}{\|(q+m)C^{\star}\|}. \tag{4.53}$$

□

Remark 1. *Note that the LMI in (4.26c) $\forall t \geq 0$ admits solution under the assumptions of Lemma 4. Indeed, when F(t) is negative definite Eq.* (2.15) *holds. Furthermore it can be numerically verified by using, for example, the interior-point method [112, 27] implemented in the Yalmip © Toolbox.*

4.4 Numerical Analysis

4.4.1 Network and Traffic Scenario

To validate the theoretical results, the proposed adaptive approach has been implemented in PLEXE [172], a high-fidelity simulator that allows the platoon investigation by coupling realistic vehicle dynamics (such

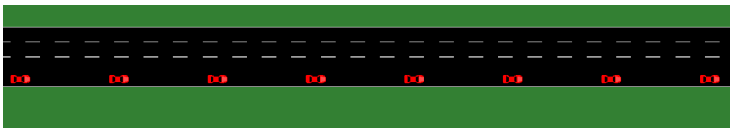


Figure 4.1: Keyframe of the simulation scenario. The vehicles platoon moves on a reserved lane (the right-most lane). Initial conditions are reported in Table 4.2.

as engine and brake limitations, air drag, friction, etc....) with realistic wireless network simulations. Indeed, PLEXE exploits, in an integrated simulation environment, the network simulator OMNeT++/MiXiM, the road traffic simulator SUMO and detailed vehicle dynamic models. OMNET++/MiXiM is used to simulate V2V communication based on the IEEE 802.11p standard, while the extended version of SUMO, that includes realistic car models, can simulate the vehicle dynamics under the action of the collaborative strategy. We remark that, in agreement with our theoretical framework we have configured the PLEXE simulator so that our collaborative algorithm only exploits neighbor information coming from V2V communications. Moreover, in this simulation environment, the different communication delays values are not parameters to be set during simulations (e.g., as well as they result from a random distribution) since their realistic presence, originated by the actual conditions of the communication channel, is accurately emulated by PLEXE [170]. To show the effectiveness of the proposed strategy for cooperative tracking, here we consider a 10 $[km]$, 3 lanes, stretch of freeway. Here an automated platoon of 7 vehicles plus a leader travels in a reserved lane (the right-most lane) and each vehicle, driven by its on-board control, has no possibility to overtake the vehicle ahead (Fig. 4.1 shows a keyframe of the simulation scenario).

The traking performances have been evaluated considering two representative leader maneuvers, namely: (i) a trapezoidal speed profile (see Fig. 4.2a); (ii) a realistic driving profile used to test the performance of connected vehicles during the Grand Cooperative Driving Challenge (GCDC) [106] (see Fig. 4.2b).

Note that the trapezoidal profiles are usually used to mimic the effect of traffic jam, when a sudden deceleration is required due to the presence of a forward obstacle (e.g. a vehicle not belonging to platoon or not

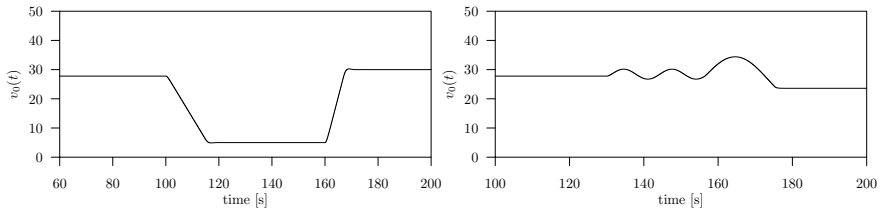


Figure 4.2: Leader maneuvers: (a) Trapezoidal speed profile; (b) Realistic driving profile.

connected) then followed by an acceleration for the repositioning of the platoon to the target velocity as soon as it is possible [59]. Furthermore, to disclose the flexibility of the approach with respect to information flows, the investigation is conducted for different exemplar communication topologies used in the platoon literature [59] and depicted in Fig. 3.5:

1. Predecessor-Follower (P-F): each vehicle can exchange information only with its preceding vehicle;

2. Leader-Predecessor-Follower (L-P-F): each vehicle can communicate with its preceding vehicle and the leading vehicle;

3. Bidirectional-Leader-Follower (B-L-F): each vehicle can exchange information with its preceding vehicle, its follower vehicle and the leading vehicle;

4. All-to-All (Broadcast, BR): each vehicle exchange information with all the other vehicles in platoon.

The parameters for both network and traffic simulation are reported in Tab. 4.1 and Tab. 4.2. Note that the value of the theoretical delay margin computed as in (4.53) and reported in Tab. 4.2, $\tau^\star = 0.21$ $[s]$, is within the average end-to-end communication delay, typical of IEEE 802.11p vehicular networks, which is of the order of hundredths of a second (i.e., 10^{-2} [s]) [6].

To further evaluate the safety in all the different driving and communication scenarios, we have also quantitatively analyzed the possible

Table 4.1: NETWORK SIMULATION PARAMETERS.

Communication system model setting	
Communication protocol	IEEE802.11p
Channel data rate	6 $[Mbps]$
Beacon frequency	10 $[Hz]$
Beacon size	200 $[bytes]$
Bernoullian channel	
PER p	0.6
Gilbert-Elliott channel	
PER p (GOOD)	0.3
PER p (BAD)	0.7
state duration	$\exp(0.5\ [s^{-1}])$ $(\mathbb{E}[X] = 2\ [s])$

Table 4.2: TRAFFIC SIMULATION PARAMETERS.

Freeway length	10 $[km]$
Lanes	3 (two-way)
Platoon size	8 cars
Platooning car max acceleration	3.5 $[ms^{-2}]$
Drivetrain constant T	0.5 $[s]$
Platooning car mass	1460 $[kg]$
Platooning car length l_{i}	4 $[m]$
Initial position $[r_0(0), \cdots, r_7(0)]^\top$	$[40, 60, 80, 100, 120, 140, 160, 180]^\top [m]$
Initial speed $[v_0(0), \cdots, v_7(0)]^\top$	$[27, 25, 22, 26, 25, 24, 28, 21]^\top$ $[ms^{-1}]$
Initial acceleration $a_i(0)$	0 $[ms^{-2}]$ $\forall i = 0, 1, \cdots, 7$
Control gains $\zeta_{ij,1}$	$\zeta_{ij,1} = 0.01$
Control gains $\zeta_{ij,2}$	$\zeta_{ij,2} = 10$
Control gains $\zeta_{ij,3}$	$\zeta_{ij,3} = 0.1$
Initial condition $\rho_{ij}(0)$	$\rho_{10}(0) = 5.9$, $\rho_{10}(0) = 2.35$
	$\rho_{i,i-1}(0) = 0.6$ $(i = 1, \cdots, N)$
Initial condition $\beta_{ij}(0)$	$\beta_{10}(0) = 6.8$, $\beta_{i0}(0) = 0.68$
	$\beta_{i,i-1}(0) = 0.68$ $(i = 1, \cdots, N)$
Initial condition $\gamma_{ij}(0)$	$\gamma_{10}(0) = 0.68$, $\gamma_{i0}(0) = 0.68$
	$\gamma_{i,i-1}(0) = 0.68$ $(i = 1, \cdots, N)$
Spacing policy d_{ij}	15 $[m]$
Theoretical delay margin $\tau^\star$	0.21 $[s]$

emergence of critical driving situations for all the maneuvers under investigation by exploiting a non-dimensional warning index (or collision index CI) that is well known in the automotive literature [138]. This index represents the occurrence of a possible physical collision in the

current driving situation and it is defined for each vehicle i ($i = 1, \cdots, 7$) as follows:

$$CI_i = \frac{c_i - d_{br,i}}{d_{w,i} - d_{br,i}} , \tag{4.54}$$

where c_i is the actual spacing between vehicle i and vehicle $i-1$; $d_{w,i}$ and $d_{br,i}$ are the braking-critical and warning-critical distances between vehicle i and vehicle $i-1$, respectively. (See [138] for the definition of all these quantities and for details on how they can be computed according to a given trajectory.) From (4.54) it follows that, if the actual distance c_i exceeds $d_{w,i}$ and $d_{br,i}$, then the warning index CI_i assumes a positive value and indicates that the current driving situation is in a safe region. If c_i is below $d_{br,i}$, then the warning index assumes a negative value denoting a dangerous driving situation. Therefore, the distance of the index from zero can be interpreted as a safety margin.
Finally, the robustness with respect to packet losses/hard delay has been also evaluated by implementing the well-known Bernoulli and Gilbert-Elliot channel models [169]. In particular, we first use a Bernoullian channel with independent random losses Packet Error Rates (PERs), and then we employ a Gilbert-Elliott channel driven by a two-state Markov chain.

4.4.2 Tracking performance for L-P-F topology

Firstly we start considering, as a preliminary analysis, the transient performance of the platoon during the special case of platoon creation. As depicted in Fig. 4.3, moving from different initial conditions among vehicles, the platoon is then engaged at $t = 50$ $[s]$ when vehicles start to move with the constant velocity imposed by the leading vehicle with a formation that preserves the spacing policy requirements. Note that all vehicles converge toward the desired mutual positions (see Fig. 4.3a) and reach the required constant speed (Fig. 4.3b). Moreover, all CI_i indexes remain strictly positive confirming that the driving situation is always safe (see Fig. 4.4).
Finally, we remark that, according to the theoretical derivation (see Theorem 5), when synchronization errors converge toward zero, adaptive gains converge toward suitable constant values with bounded dynamics (see Fig. 4.5).
Once the platoon is formed, we test the ability of the adaptive control

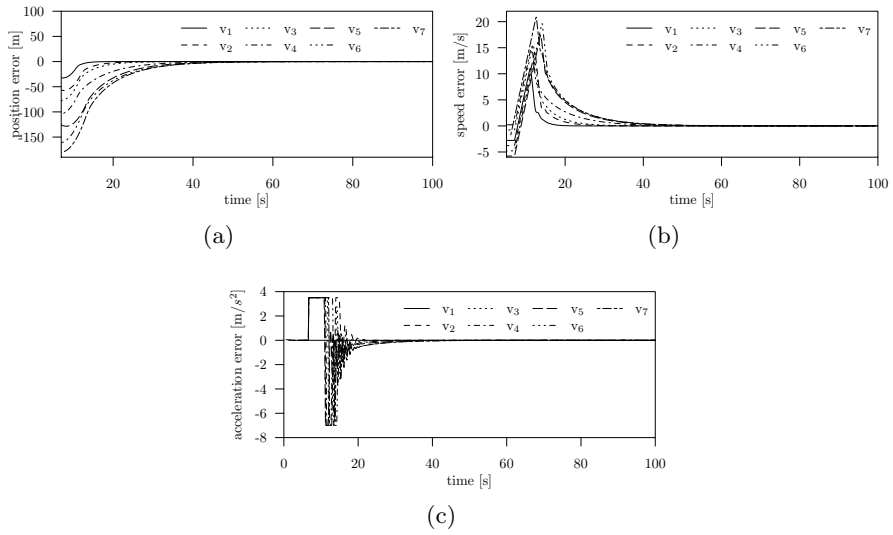


Figure 4.3: Platoon creation under L-P-F topology. Time history of the relative errors ($i = 1, \dots 7$): (a) Time history of the position error computed as $r_i(t) - r_0(t) - d_{i0}$; (b) Time history of the speed error computed as $v_i(t) - v_0$; (c) Time history of the acceleration error computed as $a_i(t) - a_0(t)$.

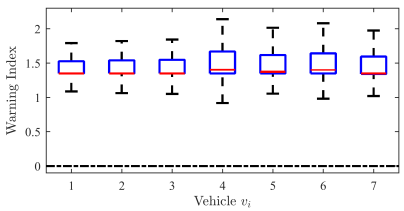


Figure 4.4: Platoon creation under L-P-F topology. Analysis of the warning index CI_i ($\forall i = 1, \cdots, 7$).

strategy in tracking the leading vehicle for the speed profile detailed in Fig. 4.2a. Specifically, at $t = 100$ $[s]$, the leader decelerates from 100 $[km\ h^{-1}]$ to 18 $[km\ h^{-1}]$ with a constant deceleration of 1.5 $[m\ s^{-2}]$; then, at $t = 160$ $[s]$, it accelerates with a constant acceleration of 3.5 $[m\ s^{-2}]$ till it reaches again the target velocity of 100 $[km\ h^{-1}]$. Results in Fig. 4.6 and Fig. 4.7 confirm the theoretical analysis and show

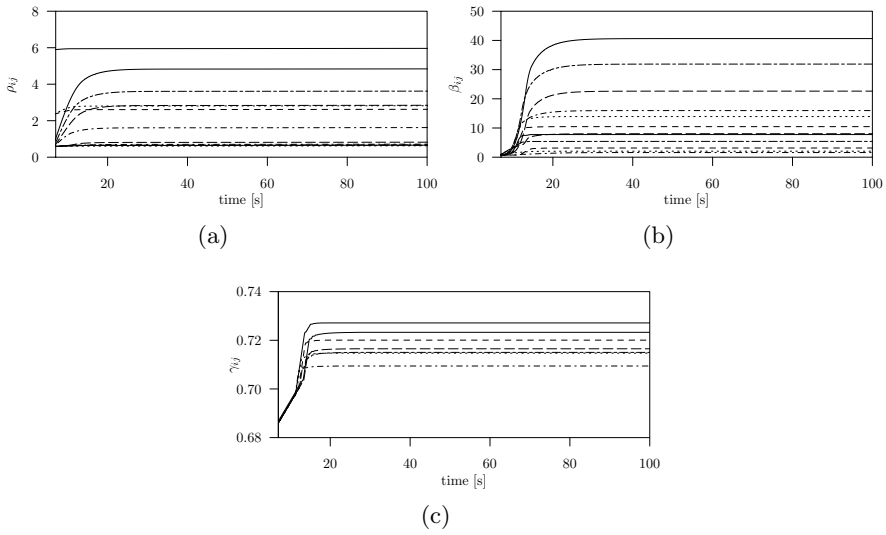


Figure 4.5: Platoon creation under L-P-F topology. Adaptive gains convergence ($i = 1, \ldots, 7$; $j = 0, \ldots, 7$): (a) Time history of the adaptive gains $\rho_{ij}(t)$; (b) Time history of the adaptive gains $\beta_{ij}(t)$; (c) Time history of the adaptive gains $\gamma_{ij}(t)$.

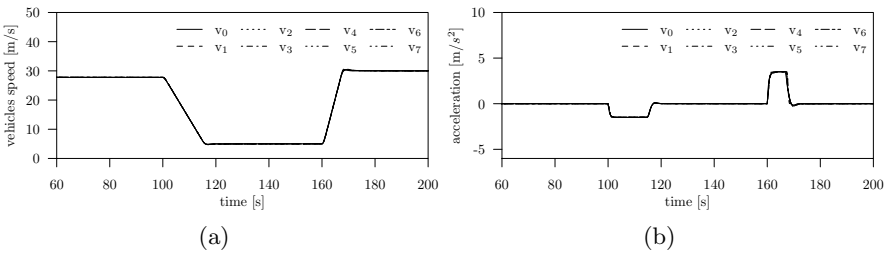


Figure 4.6: Tracking performance for the trapezoidal speed profile in Fig. 4.2a under L-P-F topology: (a) Time history of the vehicles speed $v_i(t)$ $(i = 0, \ldots 7)$; (b) Time history of the vehicles acceleration $a_i(t)$ $(i = 0, \ldots 7)$.

how vehicles safely track the leader while preserving at the same time the required mutual positions (see Fig. 4.7a). As expected, velocities and accelerations profiles in Fig. 4.6 disclose that the fast tracking

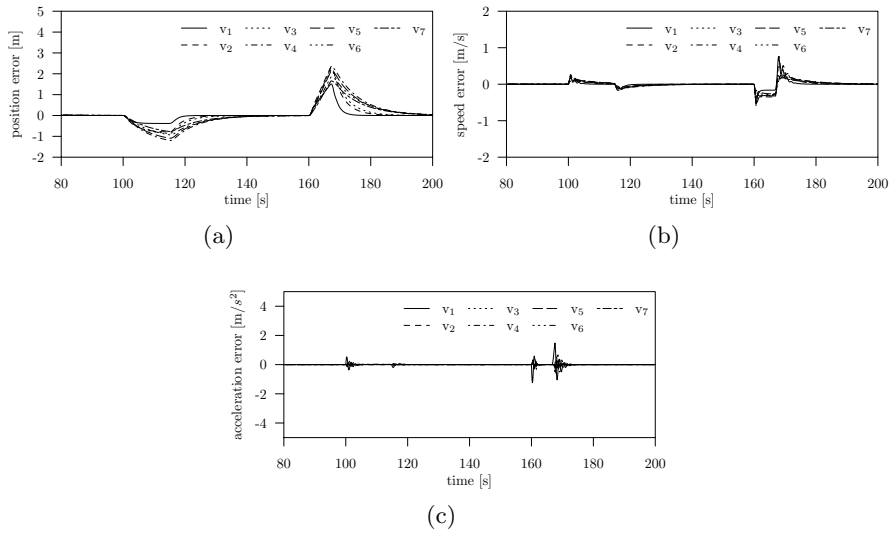


Figure 4.7: Tracking performance for the trapezoidal speed profile in Fig. 4.2a under L-P-F topology. Time histories of the relative errors ($i = 1, \dots 7$): (a) Position error computed as $r_i(t) - r_0(t) - d_{i0}$; (b) Speed error computed as $v_i(t) - v_0(t)$; (c) Acceleration error computed as $a_i(t) - a_0(t)$.

of the leader motion is achieved with a smooth behavior, while some sudden changes naturally arise in the errors profiles corresponding to transient variations in the reference velocity signal (see Fig. 4.7 and Fig. 4.2a). Note that, in order to guarantee the tracking performance, the adaptive action counteracts the synchronization errors, originated by the acceleration/deceleration of the leader, by slightly increasing the gains values (gains variations of the order of hundredths) as depicted in Fig. 4.8. Moreover, adaptive gains are always bounded during the entire maneuver. Finally, we point out that the analysis of the warning index, omitted here for the sake of brevity, reveals a safe driving situation.
The performance of the adaptive strategy have been also tested here for the realistic speed profile defined in [106]. Namely, platoon is cruising at 100 $[km\ h^{-1}]$ when the leading vehicle accelerates to 115 $[km\ h^{-1}]$ and then it brakes to 100 $[km\ h^{-1}]$. This sequence is then repeated two times. After that, at 150 $[s]$, the leader accelerates to 120 $[km\ h^{-1}]$,

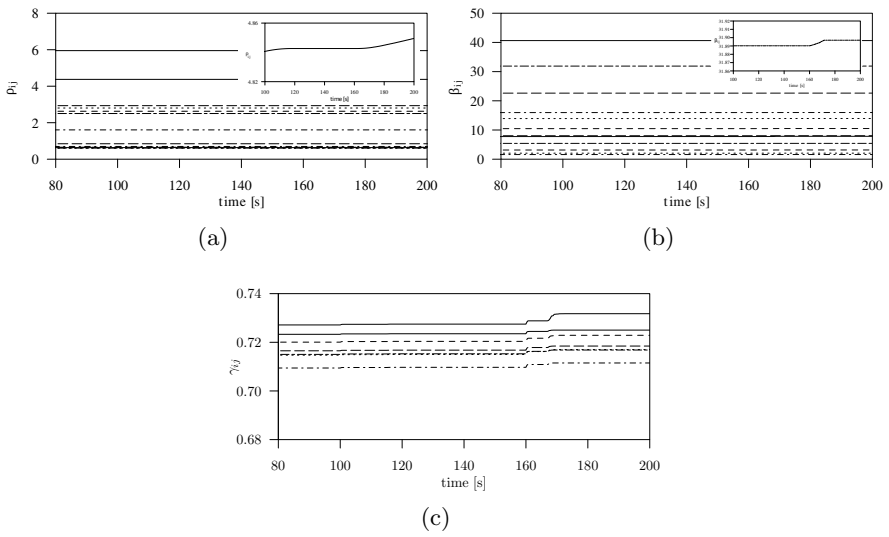


Figure 4.8: Tracking performance for the trapezoidal speed profile in Fig. 4.2a under L-P-F topology. Adaptive gains convergence ($i = 1, \ldots, 7$; $j = 0, \ldots, 7$): (a) Time history of the adaptive gains $\rho_{ij}(t)$; (b) Time history of the adaptive gains $\beta_{ij}(t)$; (c) Time history of the adaptive gains $\gamma_{ij}(t)$.

and, finally, an harsher braking is applied for approaching 85 $[km\ h^{-1}]$ (see Fig. 4.2b). Also in this case, the time history of the relative errors reported in Fig. 4.9 reveals a good cooperative tracking behavior, since each vehicle tracks the reference speed (see Fig. 4.9b) and acceleration (see Fig. 4.9c), while maintaining the rigid formation requirements (see Fig. 4.9a). Again sudden changes in the errors profiles refer to transients associated to variations in the reference signal to be tracked (see Fig. 4.2b). Furthermore, as for the previous trapezoidal maneuver, the time history of velocities and accelerations for all vehicles confirms the effectiveness of the adaptive control in tracking the leader according to the errors evolution; the CI indexes are always strictly positive during the entire maneuver; the adaptive gains turn to be bounded. Hence, the similar results have been omitted here for the sake of brevity.

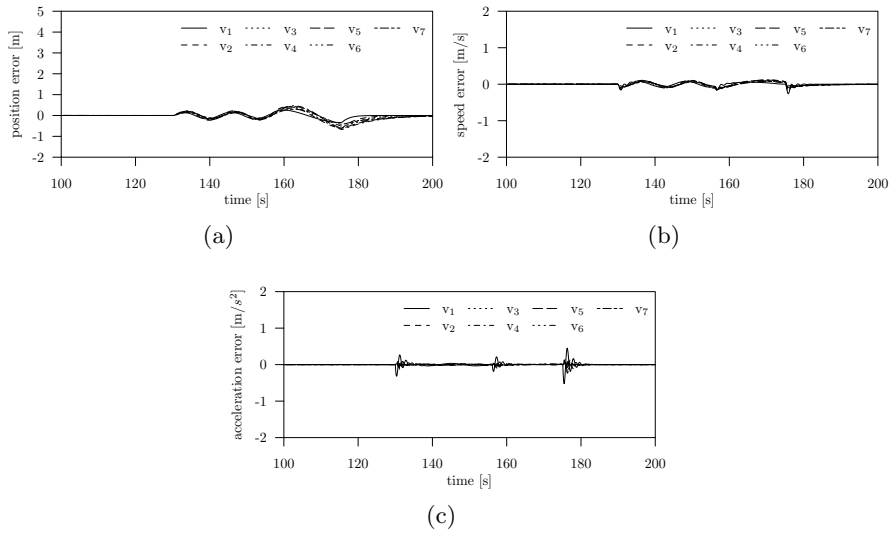


Figure 4.9: Tracking performance for the realistic driving profile in Fig. 4.2b under L-P-F topology. Time history of the relative errors ($i = 1, \ldots, 7$): (a) Time history of the position error computed as $r_i(t) - r_0(t) - d_{i0}$; (b) Time history of the speed error computed as $v_i(t) - v_0(t)$; (c) Time history of the acceleration error computed as $a_i(t) - a_0(t)$.

4.4.3 Alternative communication topologies

Good tracking performances have also been verified for alternative communication topologies. Results show that, for all topologies under investigation, the adaptive protocol is able to effectively achieve the synchronization with the leader motion, preserving at the same time the desired spacing policy within the formation. As an illustrative example, we report in Fig. 4.10 the speed profiles obtained for B-L-F (see Fig. 4.10a), BR (see Fig. 4.10b) and P-F (see Fig. 4.10c) for the trapezoidal leader maneuver depicted in Fig. 4.2a. As expected, appreciable elongations are detectable only in the case of the P-F topology depicted in Fig. 4.10c. Indeed, they are consequence of the lack of a direct communication link with the leader that introduces hard oscillations during transients as disclosed in the recent technical literature [212]. Similar results (depicted in Fig. 4.11) can be obtained for the realistic speed profiles in Fig. 4.2b.

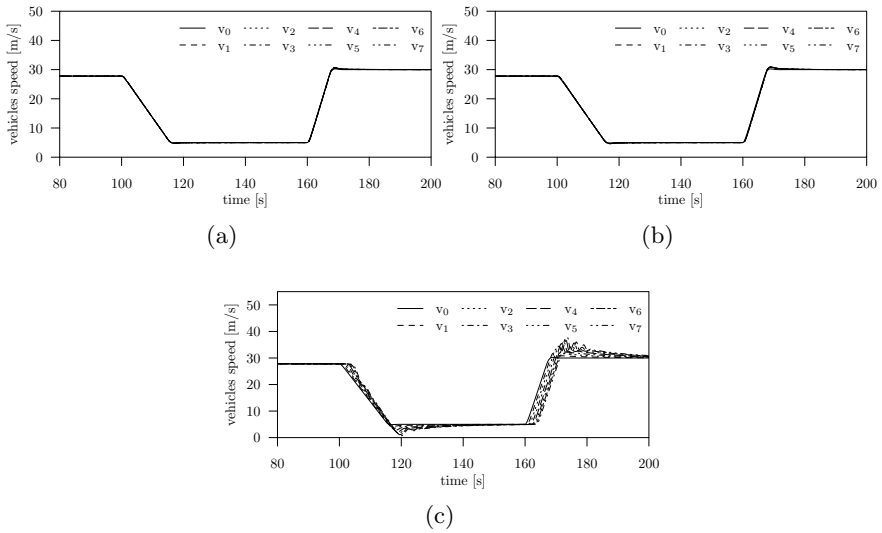


Figure 4.10: Alternative topologies. Tracking performance for the trapezoidal speed profile in Fig. 4.2a. Time history of vehicles speed, $v_i(t)$ $(i = 0, \dots 7)$: (a) B-L-F; (b) BR; (c) P-F.

We remark that, for all topologies under investigation, all gains are bounded for both the maneuvers and warning indexes always confirm the safety of the driving conditions in all the different cases. The very similar results have been hence omitted here for the sake of brevity.

4.4.4 Hard Braking maneuver for different communication topologies

To further disclose security issues, we consider here the occurrence of an hard braking (emergency) maneuver as an additional evaluation scenario. Specifically, results in Fig. 4.12 show how the platoon reacts in the case of a braking maneuver performed by the leader from 100 $[km\ h^{-1}]$ to a full stop, for each communication topology under investigation. Also in this case, the platoon correctly tracks the leader velocity during braking, till it rests, while possible collisions are avoided. To better unveil this latter aspect, we report in Fig. 4.13 the analysis of the warning index

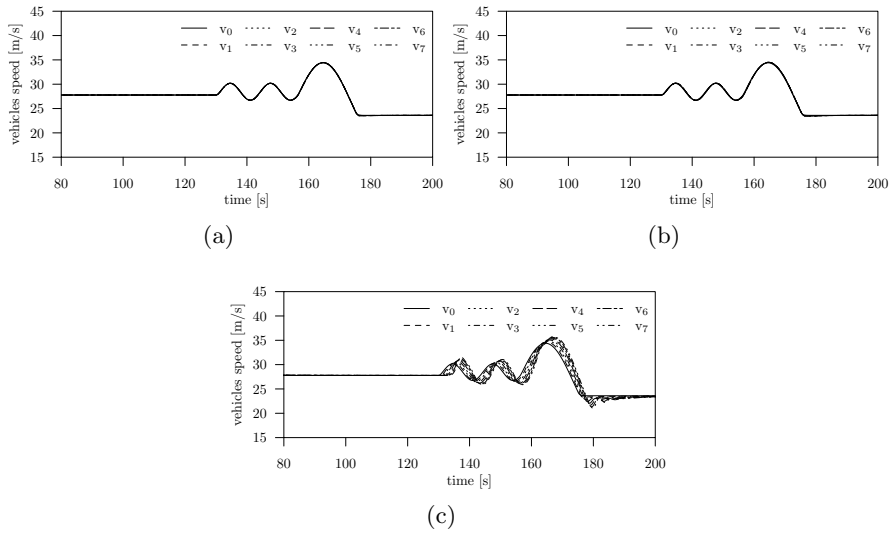


Figure 4.11: Alternative topologies. Tracking performance for the realistic driving profile in Fig. 4.2b. Time history of vehicles speed, $v_i(t)$ $(i = 0, \dots 7)$: (a) B-L-F; (b) BR; (c) P-F.

during the entire emergency maneuver for the exemplar case of the L-P-F communication topology. We point out that for all the other topologies under investigation results are very similar and, hence, they are omitted here for the sake of brevity.

4.4.5 Robustness with respect to lossy channels

Here we test the robustness of the adaptive strategy in the presence of information packet losses. We recall that, in case of packet loss, the algorithm uses the last available information, which means transmission delay actually jumps, to a large value, then returns to a smaller value when the next valid message is received. Thus the resilience to message loss, also implies the robustness to hard delay conditions.
To this aim, we consider the Bernoulli and Gilbert-Elliott channel models, whose features are reported in Tab. 4.1.
Concerning the Bernoullian channel, results in Fig. 4.14 (related to exem-

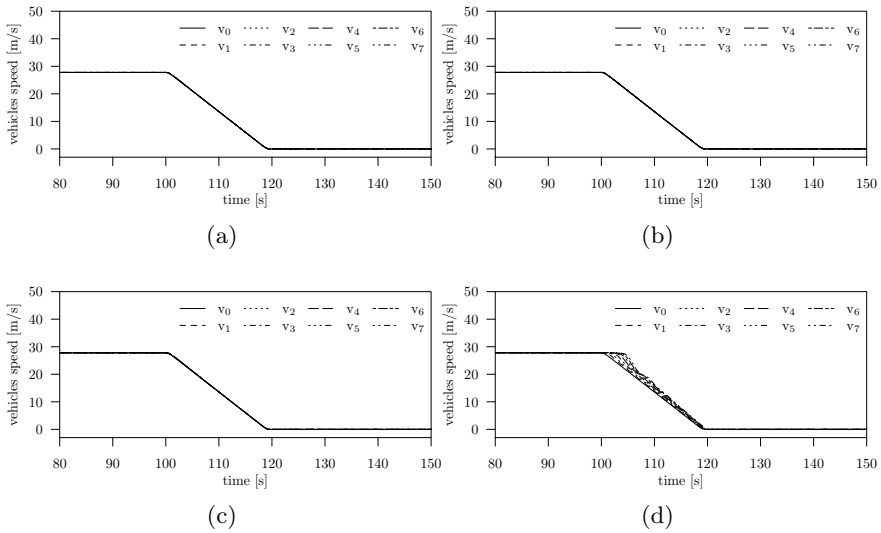


Figure 4.12: Tracking performance for a hard braking maneuver. Time history of vehicles speed, $v_i(t)$ $(i = 0, \dots 7)$: (a) L-P-F; (b) B-L-F; (c) BR; (d) P-F.

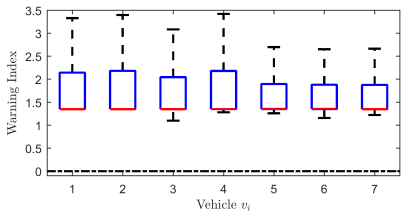


Figure 4.13: Hard braking maneuver under L-P-F topology. Analysis of the warning index CI_i $(\forall i = 1, \cdots, 7)$.

plar case of the realistic speed profile in Fig. 4.2b with L-P-F topology) show that, due to the adaptive approach that provides robustness w.r.t. uncertainties, the strategy is able to impose the reference behaviour up to PER equals to 60%. Very small position errors can be appreciated despite the hard communication impairment (Fig. 4.14). Note that boundedness of the adaptive gains is still preserved (results omitted for the sake of brevity).

Similar performances are obtained in the case of the Gilbert-Elliot chan-

nel model driven by a two-state Markov chain. Each state represents the current channel status, which can be either in good or in bad conditions (from 30% to 70% of packets lost). Results in Fig. 4.15 show that the platoon cooperatively synchronizes also in this setup and confirm the high resilience to packet losses and delays provided by adaptation (with a similar bounded behavior of the adaptive gains). Sudden changes in the position error signal (see Fig. 4.15a) are due to the occurrence of bad conditions in terms of packets lost, according to the Gilbert-Elliott transmission channel model.
We remark that similar performances can be even achieved for the other communication topologies and hence they have not been reported here for the sake of brevity.

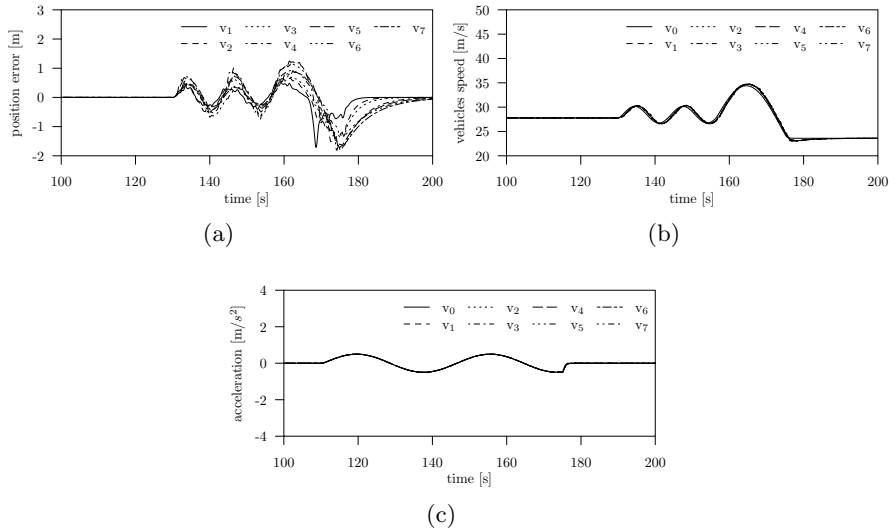


Figure 4.14: Bernoulli transmission channel. Tracking performance for the realistic driving profile in Fig. 4.2b under L-P-F topology: (a) Time history of the position error computed as $r_i(t) - r_0(t) - d_{i0}$ $(i = 1, \dots 7)$; (b) Time history of the speed $v_i(t)$ $(i = 1, \dots 7)$; (c) Time history of the acceleration $a_i(t)$ $(i = 1, \dots 7)$.

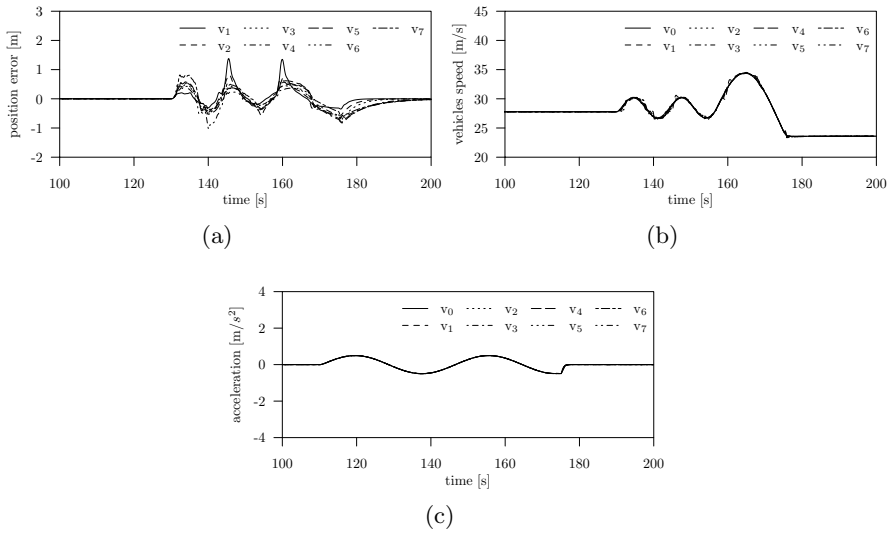
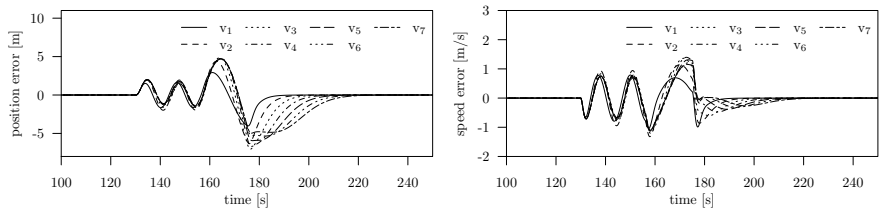


Figure 4.15: Gilbert-Elliott transmission channel. Tracking performance for the realistic driving profile in Fig. 4.2b under L-P-F topology: (a) Time history of the position error computed as $r_i(t) - r_0(t) - d_{i0}$ $(i = 1, \dots 7)$; (b) Time history of the speed $v_i(t)$ $(i = 1, \dots 7)$; (c) Time history of the acceleration $a_i(t)$ $(i = 1, \dots 7)$.

4.4.6 A Brief Comparison with an up-to-date distributed control

To better disclose the control performance, here we carry out a comparison between our distributed adaptive approach and a collaborative approach that leverages the idea of consensus [170]. Note that consensus has been recently indicated in the technical literature on interconnected vehicles as a particularly suitable tool for maintaining platoon while counteracting communication impairments (e.g., see [46] and references therein). The comparative analysis reported here has been carried out by considering, as an exemplar case, the leader maneuver depicted in Fig. 4.2b under a classical L-P-F communication topology.
Comparing the results in Fig. 4.16 with the ones depicted in Fig. 4.9, it is easy to note that, despite the good accomplishment of the consensus-

bases control, the adaptive approach achieves better performance and smaller errors. Indeed, the position error (see Fig. 4.16a) is at most equal to 5 $[m]$ and the speed error (see Fig. 4.16b) is at most 1.2 $[m\ s^{-1}]$ for the consensus-based algorithm, while smaller error values, less than 1.8 $[m]$ for positions and less than 0.8 $[m\ s^{-1}]$ for the speed, can be obtained in the case of gains adaptation (see Fig. 4.9a and Fig. 4.9b, respectively).



(a) (b)

Figure 4.16: Consensus-based controller tracking performance for the realistic driving profile in Fig. 4.2b under L-P-F topology. Time history of the relative errors ($i = 1, \dots 7$): (a): time history of the position error computed as $r_i(t) - r_0(t) - d_{i0}$; (b): time history of the speed error computed as $v_i(t) - v_0(t)$.

4.5 Concluding Remarks

The cooperative tracking problem for vehicles platoon in the presence of multiple time-varying communication delays has been investigated.
The platooning problem is solved by treating it as the problem of cooperative synchronization of LTI multi agents systems in a delayed dynamical network.
By introducing the delays related to outdated information, we proved with a Lyapunov-Krasovskii approach that the decentralized adaptive strategy can be successfully used to globally synchronize the vehicular networks to the leader dynamics.
The hi-fidelity analysis conducted with the PLEXE simulator confirmed the theoretical derivation, the robustness to uncertainties and the good responsiveness to sudden variations of the leader motion.

CHAPTER 5

On the Robustness of the distributed Adaptive Synchronization Protocol for Connected Autonomous Vehicles with Multiple Disturbances

This chapter studies the robustness property of the adaptive synchronization-based control protocol, proposed in Chapter 4, for cooperative driving of autonomous vehicles platoons in the presence of both multiple Vehicle-to-Vehicle (V2V) time-varying communication delays and external disturbances. The robust stability of the closed-loop delayed network is proven via Lyapunov-Krasovskii theory. Delay-dependent linear matrix inequalities (LMIs) conditions are analytically derived for ensuring both robust synchronization to the leader dynamics and disturbances attenuation. An exemplar driving maneuver is considered for evaluating the robustness of the performance achieved by vehicles platoon and the numerical results confirm the effectiveness of the theoretical

derivation.

5.1 Robustness Issues in Cooperative Driving Systems

Practical challenges for the deployment of autonomous connected vehicles are how to opportunely manage external disturbances acting along all the vehicular chain and communication impairments introduced by the V2V network, such as time-delays and packet losses [66]. To deal with the robustness problem w.r.t. communication impairments, consensus-based approaches have been widely investigated in [170, 97, 152] where the heterogeneity in the time-varying communication delays is investigated, though the theoretical analysis disregards leader tracking maneuvers. More recently, the leader tracking problem in the presence of multiple heterogeneous time-varying delays is addressed in [155], where an adaptive cooperative control protocol solves the issue by providing stability conditions via a Lyapunov-Krasovkii approach.
Although robustness w.r.t. delays is crucial, another fundamental requirement, however less addressed in the current platoon literature, is to provide robustness w.r.t. external disturbances arising from different environmental factors. Along this line, distributed sliding mode control [77], distributed finite-time approach [70], decentralized H_∞ controllers [215] are proposed under the ideal assumption of perfect communication. The leader tracking problem when concurrently taking into account both external disturbances and communication time-delay is instead recently addressed in [66], where a distributed H_∞ controller is designed for handling autonomous vehicles platoons under the main restrictive assumption of a homogeneous (or unique) and constant time-delay. However, in practice, communication is not perfect and, hence, each of the communication links, connecting a pair of vehicles, is affected by a different variable time-delay whose value depends on actual conditions, or possible impairments, of the communication channel [30].
Because adaptive approaches provide robustness and self-adaptivity to withstand time-varying disturbances, such as environmental factors or time-varying conditions of the communication channel, it seems suitable to solve the cooperative robust leader tracking problem via the distributed adaptive synchronization-based protocol presented in [155].

The aim of this chapter is to analytically guarantee both robust stability to uncertain external disturbances and multiple (or heterogeneous) time-varying delays, which are both present in current on-the-road driving conditions, while achieving at the same time the desired tracking performance, i.e, so that all vehicles within the platoon synchronize to the reference leading dynamics while preserving the required inter-vehicular distance. Simultaneously considering the presence of time-varying disturbances and delays, novel sufficient robustness conditions are derived and expressed as set of delay-dependent Linear Matrix Inequalities (LMIs). Theoretical results are then confirmed via numerical simulations for an exemplar driving maneuver.

5.2 Cooperative driving in uncertain driving conditions

Consider a platoon of N autonomous vehicles plus a leader moving along a single lane. The i-th generic vehicle behavior ($\forall i = 1, \ldots, N$) subject to the external disturbance is described by the following third order longitudinal model as [66, 70]:

$$\dot{x}_i = Ax_i + Bu_i(t; \tau_{ij}(t)) + Ew_i(t), \tag{5.1}$$

where $x_i(t) = [r_i(t)\ v_i(t)\ a_i(t)]^\top \in \mathbb{R}^3$ represent the i-th vehicle state vector ($i = 1, \cdots, N$) (being r_i [m] and v_i [m/s] and a_i [m/s^2] the i-th agent position (in meters), velocity (in meters per second) and acceleration (in meters per second^2), measured with respect to the road reference frame); $A \in \mathbb{R}^{3\times3}$, $B \in \mathbb{R}^{3\times1}$ are as in Eq. (4.2) while $E \in \mathbb{R}^{3\times1}$ has the following expression:

$$E = \begin{bmatrix} 0 & 0 & 1 \end{bmatrix}^\top. \tag{5.2}$$

$u_i(t; \tau_{ij}(t))$ is the distributed input providing the desired acceleration to be imposed to $i - th$ vehicle within platoon. Note that, the distributed protocol $u_i(t; \tau_{ij}(t))$ is on-board computed by handling both local measurements and the network information that are affected by time-varying delays depending on the specific communication link, i.e. $\tau_{ij}(t)$ ($j = 0, \cdots, N$) $i \neq j$. Furthermore, $w_i(t) \in \mathcal{L}_2[0; \infty)$ is the external

disturbance arising from environmental factors, such as variations in wind velocity and/or road slope.
The reference leading dynamics, not influenced by any followers and not subject to external disturbances, are instead described by the autonomous linear dynamical system as in Eq. (4.3).
To solve the cooperative leader tracking problem (see Eq. (4.4)) in the presence of multiple disturbances $w_i(t)$ acting on each vehicles dynamics i ($\forall i = 1, \dots, N$) and multiple communications delay $\tau_{i,j}(t)$ ($\forall i = 1, \dots, N;\ j = 0, 1, \dots, N,\ i \neq j$), we consider the cooperative distributed adaptive controller in Eq. (4.5) that updates its action based on the errors among the state information shared among vehicles.

5.3 Robust Stability

In this section we analytically prove the robustness of the adaptive control strategy (4.5). To this aim, we first derive the closed-loop dynamics of vehicular platoon and, then, we provide our main result according to Theorem 6 by leveraging Lyapunov-Krasovkii theory [72].

5.3.1 Closed-Loop Dynamics

Define the errors of the generic i-th and j-th vehicle with respect to leader as in Eq. (4.8) and Eq. (4.9) respectively. By recasting $u_i(t, \tau_{ij}(t))$ in terms of the state errors as in Eq. (4.10), the dynamics of the closed-loop error system for the generic i-th vehicle can be written as

$$\begin{aligned} \dot{e}_i(t) = \quad & Ae_i(t) - B\alpha_{i0}\kappa_{i0}^{\top}(t)e_i(t - \tau_{i0}(t)) + Ew_i(t) \\ & -B\sum_{j=1}^{N} \alpha_{ij}\kappa_{ij}^{\top}(t)\left[e_i(t - \tau_{ij}(t)) - e_j(t - \tau_{ij}(t))\right], \end{aligned} \tag{5.3}$$

where A-B and E are defined as in (4.2) and (5.2) respectively. Now, naming

$$-B\alpha_{i0}\kappa_{i0}^{\top}(t) = \mathcal{C}_{i0}(t) \in \mathbb{R}^{3\times 3} \quad -B\alpha_{ij}\kappa_{ij}^{\top}(t) = \widehat{\mathcal{C}}_{ij}(t) \in \mathbb{R}^{3\times 3}, \tag{5.4}$$

system (4.12) can be recast as ($i = 1, \dots, N$)

$$\begin{aligned} \dot{e}_i(t) = \quad & Ae_i(t) + Ew_i(t) + \mathcal{C}_{i0}(t)e_i(t - \tau_{i0}(t)) + \\ & \sum_{j=1}^{N} \widehat{\mathcal{C}}_{ij}(t)\left[e_i(t - \tau_{ij}(t)) - e_j(t - \tau_{ij}(t))\right]. \end{aligned} \tag{5.5}$$

Delays $\tau_{ij}(t)$ can be represented, with a more compact notation, as elements of the following delay set: $\sigma_p(t) \in \{\tau_{ij}(t) : i, j = 1, 2, ..., N, i \neq j)\}$ for $p = 1, 2, ..., m$ with $m \leq N(N-1)$. Analogously, delays $\tau_{i0}(t)$ are elements of the set: $\tau_l(t) \in \{\tau_{i0}(t) : i = 1, 2, ..., N, \}$ for $l = 1, 2, ..., q$ with $q \leq N$ [155]. Note that m and q are equal to their maximum value if the underlying network topology $\mathcal{G}_{N+1}$ is a directed complete graph and all time-delays are different.
Now, by defining the error state vector as $\widetilde{x}(t) = \left[e_1^\top(t),\ e_2^\top(t),\ \cdots,\ e_N^\top(t) \right]^\top \in \mathbb{R}^{3N}$ and the external disturbances vector as $\widetilde{w}(t) = \left[w_1^\top(t),\ w_2^\top(t),\ \cdots,\ w_N^\top(t) \right]^\top \in \mathbb{R}^N$, the dynamics of the delayed closed-loop vehicular network can be expressed as:

$$\begin{aligned} \dot{\widetilde{x}}(t) = \ & A_0\widetilde{x}(t) + \sum_{l=1}^{q} C_l(t)\widetilde{x}(t - \tau_l(t)) + \\ & \sum_{p=1}^{m} \widehat{\mathcal{C}}_p(t)\widetilde{x}(t - \sigma_p(t)) + \widetilde{E}\widetilde{w}(t) \end{aligned} \tag{5.6}$$

where $A_0 \in \mathbb{R}^{3N\times 3N}$ and $C_l(t) \in \mathbb{R}^{3N\times 3N}$ $(l = 1, \cdots, q)$ are defined as in (4.16) and (4.17) respectively; matrices $\widehat{\mathcal{C}}_p(t) \in \mathbb{R}^{3N\times 3N}$ $(p = 1, \cdots, m)$ are block matrices such that each block is given as in (4.19). Moreover, $\widetilde{E}$ is the following diagonal block matrix:

$$\widetilde{E} = \begin{bmatrix} E & 0^{3\times 1} & \cdots & 0^{3\times 1} \\ 0^{3\times 1} & E & \cdots & \vdots \\ \vdots & \vdots & \ddots & \vdots \\ 0^{3\times 1} & \cdots & \cdots & E \end{bmatrix} \in \mathbb{R}^{3N\times N}, \tag{5.7}$$

being E defined as in (5.2).
By introducing a model transformation with the Leibniz-Newton formula [28] (see Definition 4), and by naming $F(t) = A_0 + \sum_{l=1}^{q} C_l(t) + \sum_{p=1}^{m} \widehat{\mathcal{C}}_p(t) \in \mathbb{R}^{3N\times 3N}$, the delayed closed-loop system (5.6) can be finally recast as:

$$\begin{aligned} \dot{\widetilde{x}}(t) = \ & F(t)\widetilde{x}(t) - \sum_{l=1}^{q} C_l(t) \int_{t-\tau_l(t)}^{t} \dot{\widetilde{x}}(s)ds \\ & - \sum_{p=1}^{m} \widehat{\mathcal{C}}_p(t) \int_{t-\sigma_p(t)}^{t} \dot{\widetilde{x}}(s)ds \ + \widetilde{E}\widetilde{w}(t). \end{aligned} \tag{5.8}$$

5.3.2 Proof of Robust Stability

Here, we analytically prove the robust stability of the delayed closed-loop vehicular network (5.8) considering the following disturbance rejection index J for a prescribed scalar $\gamma > 0$:

$$J = \int_0^t \widetilde{x}^\top(s)\widetilde{x}(s) - \gamma^2 \widetilde{w}^\top(s)\widetilde{w}(s)ds. \tag{5.9}$$

The aim is to find stability conditions that ensure both asymptotic stability and robustness attenuation requirement guaranteeing that $J < 0$ [65, 192].
According to the delay system literature [72, 153] we assume here that delays are bounded, i.e. $\sigma_p(t) \in [0, \sigma_p^\star]$, $\dot{\sigma_p}(t) \in (0, d_p]$ $\forall t$, $\forall p$ and $d_p \leq 1$ and $\tau_l(t) \in [0, \tau_l^\star]$, $\dot{\tau_l}(t) \in (0, d_l]$ $\forall t$, $\forall l$ and $d_l \leq 1$. Note that, this assumption fits for the technological constraints of V2V communication, where delays are bounded in practice [6].
Now, delay-dependent robust stability conditions can be expressed as a Linear Matrix Inequality (LMI) criterion according to the following Theorem.

Theorem 6. *Consider the delayed closed-loop vehicular network (5.8) under the action of the distributed adaptive control protocol (4.5). Assume delays $\tau_l(t)$ $(l = 1, \ldots, q)$ and $\sigma_p(t)$ $(p = 1, \ldots, m)$ to be bounded and node 0 to be globally reachable in $\mathcal{G}_{N+1}$.*
If there exist the following positive definite matrices P, Q_l, Q_p, M_l, $\widetilde{M}_p \in \mathbb{R}^{3N\times 3N}$ and a scalar $\gamma > 0$, such that the following LMIs hold:

$$F^\top(t)P + PF(t) + \sum_{l=1}^{q} Q_l + \sum_{p=1}^{m} Q_p + A_0^\top N A_0 + I^{3N\times 3N} < 0 \tag{5.10a}$$

$$C_l^\top(t)NC_l(t) - Q_l(1 - d_l) < 0, \tag{5.10b}$$

$$\widehat{\mathcal{C}}_p^\top(t)N\widehat{\mathcal{C}}_p(t) - Q_p(1 - d_p) < 0, \tag{5.10c}$$

$$\widetilde{E}^\top N\widetilde{E} - \gamma^2 I^{N\times N} < 0, \tag{5.10d}$$

being $N = \sum_{l=1}^{q} \tau_l^\star M_l + \sum_{p=1}^{m} \sigma_p^\star \widetilde{M}_p$, then the delayed vehicular network (5.8) achieves synchronization as in (4.4) and it is also robust stable w.r.t. external disturbances, i.e.

$$\lim_{t\to\infty} \widetilde{x}(t) = 0 \quad J(\widetilde{w}) < 0. \tag{5.11}$$

Moreover, adaptive gains in (4.7) converge to a constant value $\kappa_{ij}^{\star} \in \mathbb{R}^3 (\forall i = 1, \ldots, N \; j = 0, 1, \ldots, N)$.

Proof. Consider the following Lyapunov-Krasovkii functional:

$$\begin{aligned} V(\widetilde{x}(t)) = \; & \widetilde{x}^{\top}(t) P \widetilde{x}(t) + \sum_{l=1}^{q} \int_{t-\tau_l(t)}^{t} \widetilde{x}^{\top}(s) Q_l \widetilde{x}(s) ds \\ & + \sum_{p=1}^{m} \int_{t-\sigma_p(t)}^{t} \widetilde{x}^{\top}(s) Q_p \widetilde{x}(s) ds \\ & + \sum_{l=1}^{q} \int_{-\tau_l^{\star}}^{0} \int_{t+\theta}^{t} \dot{\widetilde{x}}(s)^{\top} M_l \dot{\widetilde{x}}(s) ds d\theta \\ & + \sum_{p=1}^{m} \int_{-\sigma_p^{\star}}^{0} \int_{t+\theta}^{t} \dot{\widetilde{x}}(s)^{\top} \widetilde{M}_p \dot{\widetilde{x}}(s) ds d\theta \end{aligned} \tag{5.12}$$

where P, Q_l, Q_p, M_l and $M_p \in \mathbb{R}^{3N \times 3N}$ are constant symmetric and positive definite matrices to be determined.
Differentiating $V(\widetilde{x}(t))$ along the trajectories of the closed-loop system (5.8), given the bounds on delays, we have:

$$\begin{aligned} \dot{V}(\widetilde{x}(t)) \leq \; & \widetilde{x}^{\top}(t) \left(F^{\top}(t) P + P F(t) \right) \widetilde{x}(t) \\ & - 2 \widetilde{x}^{\top}(t) P \sum_{l=1}^{q} C_l(t) \int_{t-\tau_l^{\star}}^{t} \dot{\widetilde{x}}(s) ds \\ & - 2 \widetilde{x}^{\top}(t) P \sum_{p=1}^{m} \widehat{\mathcal{C}}_p(t) \int_{t-\sigma_p^{\star}}^{t} \dot{\widetilde{x}}(s) ds + 2 \widetilde{x}^{\top}(t) P \widetilde{E} \widetilde{w}(t) \\ & + \sum_{l=1}^{q} \widetilde{x}^{\top}(t) Q_l \widetilde{x}(t) - \sum_{l=1}^{q} \widetilde{x}^{\top}(t - \tau_l(t)) Q_l \left(1 - d_l\right) \widetilde{x}(t - \tau_l(t)) \\ & + \sum_{p=1}^{m} \widetilde{x}^{\top}(t) Q_p \widetilde{x}(t) \\ & - \sum_{p=1}^{m} \widetilde{x}^{\top}(t - \sigma_p(t)) Q_p \left(1 - d_p\right) \widetilde{x}(t - \sigma_p(t)) \\ & + \dot{\widetilde{x}}(t) \sum_{l=1}^{q} \tau_l^{\star} M_l \dot{\widetilde{x}}(t) - \sum_{l=1}^{q} \int_{t-\tau_l^{\star}}^{t} \dot{\widetilde{x}}^{\top}(s) M_l \dot{\widetilde{x}}(s) ds \\ & + \dot{\widetilde{x}}(t) \sum_{p=1}^{m} \sigma_p^{\star} \widetilde{M}_p \dot{\widetilde{x}}(t) - \sum_{p=1}^{m} \int_{t-\sigma_p^{\star}}^{t} \dot{\widetilde{x}}^{\top}(s) \widetilde{M}_p \dot{\widetilde{x}}(s) ds. \end{aligned} \tag{5.13}$$

Let $N = \sum_{l=1}^{q} \tau_l^{\star} M_l + \sum_{p=1}^{m} \sigma_p^{\star} \widetilde{M}_p$ and

$$\begin{aligned} \xi(t) = \; & \big[\tilde{x}^{\top}(t), \tilde{x}^{\top}(t - \tau_1(t)), \ldots, \tilde{x}^{\top}(t - \tau_q(t)), \\ & \tilde{x}^{\top}(t - \sigma_1(t)), \ldots, \tilde{x}^{\top}(t - \sigma_m(t)), \widetilde{w}(t) \big]^{\top} \in \mathbb{R}^{\upsilon}, \end{aligned} \tag{5.14}$$

being $\upsilon = (1+m+q)3N+N$.
Taking into account (5.14) and (5.6), after some algebraic manipulations, inequality (5.13) can be rewritten as:

$$\begin{aligned}\dot{V}(\widetilde{x}) \leq \;& \xi^{\top}(t)\Phi(t)\xi^{\top}(t) - 2\widetilde{x}^{\top}(t)P\sum_{l=1}^{q} C_l(t)\int_{t-\tau_l^{\star}}^{t}\dot{\widetilde{x}}(s)ds \\ & -2\widetilde{x}^{\top}(t)P\sum_{p=1}^{m}\widehat{\mathcal{C}}_p(t)\int_{t-\sigma_p^{\star}}^{t}\dot{\widetilde{x}}(s)ds - \sum_{l=1}^{q}\int_{t-\tau_l^{\star}}^{t}\dot{\widetilde{x}}^{\top}(s)M_l\dot{\widetilde{x}}(s)ds \\ & -\sum_{p=1}^{m}\int_{t-\sigma_p^{\star}}^{t}\dot{\widetilde{x}}^{\top}(s)\widetilde{M}_p\dot{\widetilde{x}}(s)ds,\end{aligned} \tag{5.15}$$

being $\Phi(t) \in \mathbb{R}^{\upsilon\times\upsilon}$ the matrix defined Fig. 5.1 whose diagonal blocks, $\varphi_{i,i}(t) \in \mathbb{R}^{3N\times 3N}$, are given as

$$\begin{cases}\varphi_{(1,1)}(t) = F^{\top}(t)P + PF(t) + \sum_{l=1}^{q} Q_l + \sum_{p=1}^{m} Q_p + A_0^{\top}NA_0, \\ \varphi_{(l+1,l+1)}(t) = C_l^{\top}(t)NC_l(t) - Q_l(1-d_l), \\ \varphi_{(q+p+1,q+p+1)}(t) = \widehat{\mathcal{C}}_p^{\top}(t)N\widehat{\mathcal{C}}_p(t) - Q_p(1-d_p),\end{cases} \tag{5.16}$$

with $l = 1,\ldots,q$; $p = 1,\ldots,m$.

Now, defining the following augmented vector as in [177]

$$\Phi(t) = \begin{bmatrix} \varphi_{1,1}(t) & 2A_0^{\top}NC_1(t) & \cdots & \cdots & 2A_0^{\top}NC_q(t) & 2A_0^{\top}N\widehat{\mathcal{C}}_1(t) & \cdots & 2A_0^{\top}H_1\widehat{\mathcal{C}}_m(t) & 2P\widetilde{E}+2A_0^{\top}N\widetilde{E} \\ 0^{3N\times 3N} & \varphi_{2,2}(t) & 2C_1^{\top}(t)NC_2(t) & \cdots & 2C_1^{\top}(t)NC_q(t) & 2C_1^{\top}(t)N\widehat{\mathcal{C}}_1(t) & \cdots & 2C_1^{\top}(t)N\widehat{\mathcal{C}}_m(t) & 2C_1^{\top}(t)N\widetilde{E} \\ \vdots & 0^{3N\times 3N} & \ddots & \ddots & \cdots & \cdots & \cdots & \vdots & \vdots \\ \vdots & \vdots & \ddots & \ddots & 2C_q^{\top}(t)N\widehat{\mathcal{C}}_1(t) & \cdots & \cdots & \vdots & 2C_q^{\top}(t)N\widetilde{E} \\ \vdots & \vdots & \vdots & \ddots & \varphi_{q+1,q+1}(t) & 2\widehat{\mathcal{C}}_1^{\top}(t)N\widehat{\mathcal{C}}_2(t) & \vdots & \vdots & 2\widehat{\mathcal{C}}_1^{\top}(t)N\widetilde{E} \\ \vdots & \vdots & \cdots & \ddots & 0^{3N\times 3N} & \varphi_{q+2,q+2}(t) & \ddots & \vdots & \vdots \\ \vdots & \vdots & \cdots & \cdots & \cdots & 0^{3N\times 3N} & \ddots & 2\widehat{\mathcal{C}}_{m-1}^{\top}(t)N\widehat{\mathcal{C}}_m(t) & \vdots \\ 0^{3N\times 3N} & \cdots & \cdots & \cdots & \cdots & \cdots & 0^{3N\times 3N} & \varphi_{q+m+1,q+m+1}(t) & 2\widehat{\mathcal{C}}_m^{\top}(t)N\widetilde{E} \\ 0^{N\times 3N} & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & 0^{N\times 3N} & \widetilde{E}^{\top}N\widetilde{E} \end{bmatrix}$$

Figure 5.1: $\Phi(t) \in \mathbb{R}^{\upsilon\times\upsilon}$

$$\begin{aligned}\zeta(t) = \;& \Big[\xi(t), \int_{t-\tau_1^{\star}}^{t}\dot{\widetilde{x}}^{\top}(s),\ldots,\int_{t-\tau_q^{\star}}^{t}\dot{\widetilde{x}}^{\top}(s), \int_{t-\sigma_1^{\star}}^{t}\dot{\widetilde{x}}^{\top}(s),\ldots, \\ & \int_{t-\sigma_m^{\star}}^{t},\dot{\widetilde{x}}^{\top}(s)\Big]^{\top} \in \mathbb{R}^{\nu}\end{aligned} \tag{5.17}$$

where $\nu = \upsilon + (m+q)3N$, it is possible to recast inequality (5.15) in a more compact form as:

$$\dot{V}(\widetilde{x}) \leq \zeta^{\top}(t)\Theta(t)\zeta(t) \tag{5.18}$$

being $\Theta(t) \in \mathbb{R}^{\nu \times \nu}$ the following diagonal block matrix:

$$\left[\begin{array}{c|c} \Phi(t) & \begin{array}{cccccc} -2PC_1(t) \cdots & -2PC_q(t) & -2P\widehat{\mathcal{C}}_1(t) & \cdots & -2P\widehat{\mathcal{C}}_m(t) \\ 0^{3N\times 3N} \ \ldots & \ldots & \ldots & \ldots & \ldots & 0^{3N\times 3N} \\ \vdots \quad \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0^{3N\times 3N} \ \ldots & \ldots & \ldots & \ldots & \ldots & 0^{3N\times 3N} \end{array} \\ \hline 0^{(m+q)3N\times(m+q)3N} & \begin{array}{cccccc} -M_1 & 0^{3N\times 3N} & \ldots & \ldots & \ldots & 0^{3N\times 3N} \\ 0^{3N\times 3N} & \ddots & \ddots & \vdots & \vdots & \vdots \\ \vdots & \ddots & -M_q & \ddots & \vdots & \vdots \\ \vdots & \ldots & \ddots & -\widetilde{M}_1 & \ddots & \vdots \\ \vdots & \ldots & \ldots & \ddots & \ddots & 0^{3N\times 3N} \\ 0^{3N\times 3N} & \ldots & \ldots & \ldots & 0^{3N\times 3N} & -\widetilde{M}_m \end{array} \end{array}\right]. \tag{5.19}$$

Given the attenuation index J as in (5.9), following [65, 192] robust synchronization is guaranteed if

$$\zeta^\top(t)\Theta(t)\zeta(t) + \widetilde{x}^\top(t)\widetilde{x}(t) - \gamma^2\widetilde{w}^\top(t)\widetilde{w}(t) < 0, \tag{5.20}$$

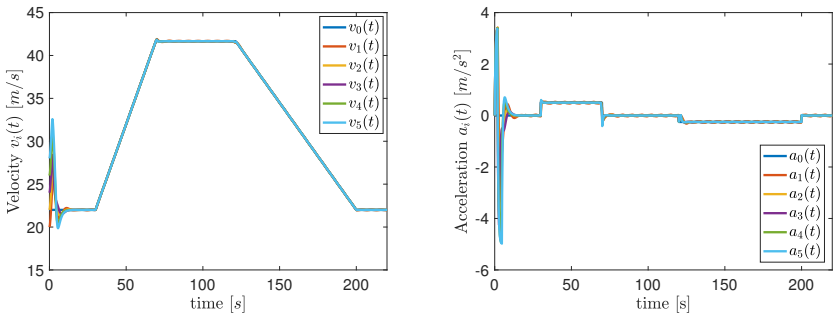
and, hence, if the LMIs in (5.10) hold. Now, following the approach in [173], from the fulfillment of (5.20), by integrating equations (4.7), it is possible to prove that all $\kappa_{ij}(t)$ tend to some constant values $\kappa_{ij}^\star$. In so doing the statement is proven. □

Remark 2. *The assumption of globally reachability of the leader guarantees that the matrix $F(t)$ is negative definite (see Lemma 4) and, hence, that LMIs in (5.10) are feasible $\forall t \geq 0$.*

Remark 3. *The LMIs in (5.10) can be numerically solved by using the interior-point method [27] implemented in the Yalmip© Toolbox.*

5.4 Numerical Validation

In this section, the robustness of the distributed adaptive control strategy (4.5) is disclosed by considering an exemplar platoon of five vehicles plus a leader connected through an exemplar Leader-Predecessor-Follower (L-P-F) [218] topology. Note that, although many different communication



(a) (b)

Figure 5.2: Leader tracking driving maneuver: a) time history of the vehicle velocity $v_i(t)$ $(i = 0, 1, 2, 3, 4, 5)$; b) time history of the vehicle acceleration $a_i(t)$ $(i = 0, 1, 2, 3, 4, 5)$.

topologies may arise for platooning, according to the V2V paradigm, the appraised L-P-F structure has been chosen as meaningful illustrative case study since it is very common in the technical automotive literature (see [218] and references therein). The numerical analysis have been performed by exploiting the MATLAB© platform where, for the simulation scenario, communication delays have been emulated as a time-varying functions whose maximum value, i.e. $\tau_l^\star = \sigma_p^\star = 0.1$ $[s]$, is set above the typical value observed in practice for IEEE 802.11p vehicular networks (which is of the order of few hundredths of a second, i.e. 10^{-2} $[s]$ [6]). Moreover, according to [70], we consider sinusoidal disturbances with different amplitudes acting on each of the platoon members, i.e., $w_i(t) = A_i \sin(t)$, for $t \geq 20$ $[s]$. Simulation parameters are reported in Tab. 4.2. Results are related to an illustrative leader tracking trapezoidal maneuver. Specifically, the leader, traveling with an initial velocity of 22 $[m/s]$, begins to accelerate at time $t =$ 30 $[s]$ with a constant acceleration of 0.5 $[m/s^2]$ until it reaches a constant velocity of 42 $[m/s]$. Then, at time $t =$ 120 $[s]$ it starts to decelerate with a deceleration of -0.25 $[m/s^2]$ until it achieves a final constant velocity equal to 22 $[m/s]$. According to the theoretical derivation in Section 5.3, results, reported in Figs. 5.2 and 5.3, reveal the ability of the proposed distributed controller in guaranteeing the required platooning formation despite the external disturbances, acting on vehicle dynamics. and the

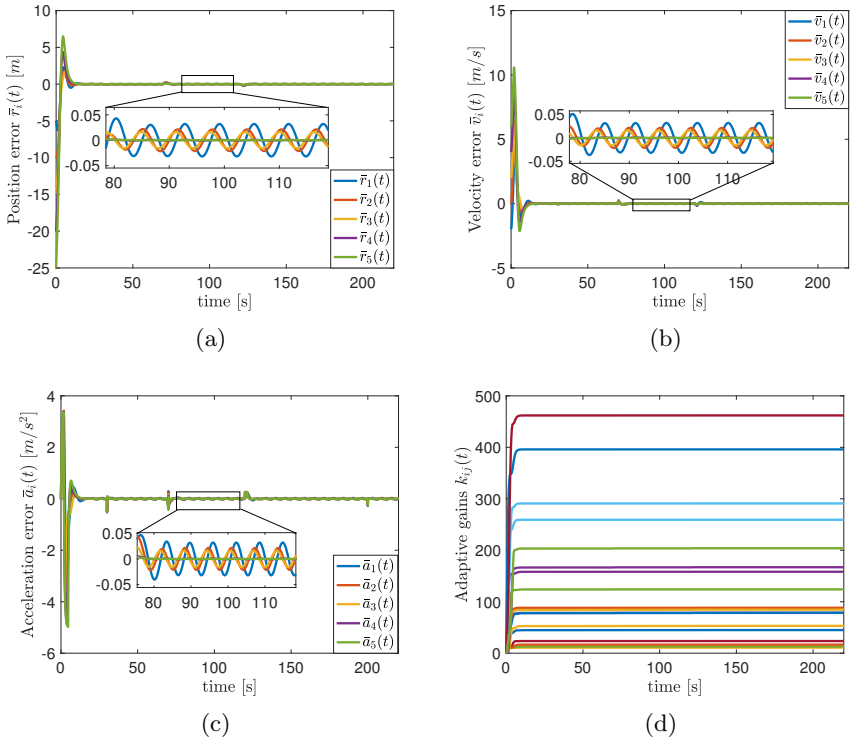


Figure 5.3: Leader tracking driving maneuver: a) time history of the position error $\bar{r}_i(t)$, computed as $r_i(t) - r_0(t) - d_{i0}$ $(i = 1, 2, 3, 4, 5)$; b) time history of the velocity error $\bar{v}_i(t)$, computed as $v_i(t) - v_0(t)$ $(i = 1, 2, 3, 4, 5)$; c) time history of the acceleration error $\bar{a}_i(t)$, computed as $a_i(t) - a_0(t)$ $(i = 1, 2, 3, 4, 5)$; d) time history of the adaptive gains $\kappa_{ij}(t)$.

time-varying delays, affecting the V2V communication. Indeed, all vehicles track the leader behavior (see Figs. 5.2a and 5.2b) while preserving the desired inter-vehicular distance $d_{i,j}$ $(\forall i = 1, \ldots, 5, j = 0, 1, \ldots, 5)$ (see Fig. 5.3a). Note that, as depicted in Figs. 5.3a, 5.3b and 5.3c, all external disturbances are strongly attenuated (more than 95%) and hence just some very small bounded errors can be observed. Finally, we remark that, coherently with the theoretical results (in Theorem 6), the adaptive gains are always bounded and converge toward suitable constant values

when synchronization errors converge to zero (see Fig. 5.3d).

5.5 Concluding Remarks

The robustness of a distributed adaptive cooperative synchronization-based protocol for a platoon of connected vehicles in the presence of multiple time-varying communication delays and external disturbances has been investigated. The robust stability of the uncertain closed-loop vehicular network has been proved through the Lyapunov-Krasovksii approach, thus yielding to delay-dependent stability conditions expressed as a set of feasible LMIs. Results disclose that the distributed adaptive strategy can be successfully used to globally synchronize the vehicular platoon to the leader dynamics, while attenuating external disturbances acting on the vehicles platoon. Exemplary numerical simulations confirm the effectiveness of the controller in guaranteeing the robust cooperative tracking.

CHAPTER 6

Distributed Resilient Control strategy for autonomous connected vehicles platoons in presence of security vulnerabilities

The Vehicular ad hoc Networks and the de facto vehicular networking standard IEEE 802.11p communication protocol are key tools for the deployment of platooning applications, since the cooperation among vehicles is based on a reliable communication structure. However, vehicular networks can suffer different security threats. Indeed, in collaborative driving applications, the sudden appearance of a malicious attack can mainly compromise: i) the correctness of data traffic flow on the vehicular network by sending malicious messages that alter the platoon formation and its coordinated motion; ii) the safety of platooning application by altering vehicular network communication capability. In view of the fact that cyber attacks can lead to dangerous implications for the security of

autonomous driving systems, it is fundamental to consider their effects on the behavior of the interconnected vehicles, and to try to limit them from the control design stage.
To this aim, in this chapter we focus on some relevant types of malicious threats that affect the platoon safety, i.e. application layer attacks (Spoofing and Message Falsification) and network layer attacks (Denial of Service and Burst Transmission), and we propose a novel collaborative control strategy for enhancing the protection level of autonomous platoons. The control protocol is designed and validated in both analytically and numerically way, for the appraised malicious attack scenarios and for different communication topology structures. The effectiveness of the proposed strategy is shown by using PLEXE, a state of the art inter-vehicular communications and mobility simulator that includes basic building blocks for platooning. A detailed simulation analysis discloses the robustness of the proposed approach and its capabilities in reacting to the malicious attack effects.

6.1 Security Issues in Cooperative Driving Systems

Most studies on vehicles platooning focus their attention on the control strategy design [158, 167, 155, 60] under the main assumption that the communication structure is reliable. In this chapter, instead, we consider an autonomous platoon of N vehicles traveling on a single lane and sharing information through a non reliable V2V wireless communications, in order to achieve cooperative driving. Indeed, similarly to other open and dynamic networks, vehicular ad hoc networks are affected by different security threats [103]. In these networks a cyber attack can lead to dangerous implication for safety, privacy and, moreover, for the public perception and consideration of vehicles platoon [79].
Countless studies on security issues in VANETs are presented in [159, 26, 5, 141, 201, 121], where several tools, helpful in building a secure vehicular network, have been exposed. One of the most proposed solution consists in exploiting authentication/validation mechanism for the messages exchanged among vehicles in order to remove from communication network the adversary, disabling its communication capability. In addiction, the works [94, 4, 134] present an accurate

categorization of all the possible malicious attacks on VANETs and of the eventual countermeasures allowing their prevention.
Although all these aforementioned works discuss the cyber attacks implications and propose network layer countermeasures, none of them considers the effects of malicious attacks on vehicular networks of connected vehicles equipped with a longitudinal control. Only recently, the security vulnerabilities problem on vehicles platooning has been addressed in [75, 124, 11, 78, 23, 13, 40, 67, 44]. These works suggest how important is, in control protocol design, to take into account the eventual cyber attacks on vehicular platooning network in order to improve its safety. Indeed, while security in sensing and communication has been extensively investigated in the technical literature, security in control has been recently indicated as a key ingredient that has to be added for enhancing the protection level of the normal operation of a physical process (e.g. see [75, 124]).
Motivated by this reason, we focus our attention on different situations in which the correct communication among autonomous vehicles is compromised and, based on this analysis, we propose a novel distributed collaborative strategy that guarantees the platoon formation in adversarial environment and that allows to promptly react to malicious attacks. The proposed distributed control approach also leverages a real-time voting technique to achieve the complete mitigation of some of the most critical effects due to malicious attacks.
This does not imply that we aim to substitute other solutions for security, such as the cryptographic ones [121] that work at the information level to avoid that the content of the information can be somehow altered. Our aim is to provide further countermeasures to detect, mitigate and, if possible, counteract cyber threats that may alter driving decision at control level so to help increasing the overall security of the ensemble of the connected vehicles.
Moreover, besides cyber attacks we also consider that each communication link, that connects a pair of vehicles, is affected by a different time-delay that accounts for actual conditions, or possible impairments, of the communication channel.
The main contribution of this work is twofold. First, differently from literature, we propose a collaborative control strategy specifically designed both to take into account cyber threats, as messages manipulation

attacks and communication capability attacks and communication impairments. The proposed approach is, hence, able to guarantee the cooperative driving of the vehicles platoon in the presence of malicious attack on the communication network as well as communication time-delay by promptly counteracting them.
Second, the proposed collaborative strategy is implemented in PLEXE [172], and we carry out a comprehensive experimental analysis with eight cars in a realistic highway (10 km long) considering different cyber attacks scenarios and different communication network topologies in which the leading vehicle is globally reachable. The communication delay in the control protocol, instead, is intrinsically modeled in Veins with a realistic communications device (IEEE 802.11p card) implementation [180]. The simulation analysis shows the main security vulnerabilities effects on the platoon motion and illustrates the robustness of the collaborative control strategy with respect to the most common malicious attacks.

6.2 Cyber Attacks in Vehicular Network

The literature on cyber attacks to vehicular networks is both wide and variegate. In this section, first we focus our attention on attacks to vehicular networks of interest for platooning, then we focus on countermeasures for this application scenario.

6.2.1 Malicious Attacks to Vehicular Networks

Here, we provide an overview of the most relevant types of malicious threats that may compromise the functionalities of cooperative driving systems (e.g., see [11], [84, 56] and references therein). Indeed, with respect to autonomous driving applications, a malicious node can affect: i) the correct data traffic flow by sending malicious messages; ii) the safety by altering vehicular network communication capability; iii) the vehicle privacy by listening to legitimate messages. Before introducing different cyber security scenarios, we first define the adversary typology [160]. An adversary can be an insider, i.e. an authenticated member of the network possessing a certified public key, or an outsider, i.e. a

network intruder. If the adversary does not get benefit from the attack, but it aims to harm the network members, it is said malicious, while it is defined rational if it seeks personal benefit. Furthermore, the adversary is defined active if it generates packet or signals, whereas it is defined passive if it realizes an eavesdropping attack.
In our vehicular scenario, application layer attacks affect the correct operating of the cooperative driving by altering the messages exchanged among vehicles to reach and maintain a common motion. Specifically, in a spoofing attack the adversary impersonates a vehicle, or more than one vehicle, in the platoon taking the control of the vehicle itself or injecting fraudulent information. Instead, in a message falsification attack, an adversary starts listening the messages wirelessly sent on networks and, after receiving each beacon, it tries to manipulate and to falsify the content of messages in order to rebroadcast them. Value changing of messages beacon field could have different effects depending on the implementation of the vehicle control strategy. For example, an alteration of the position beacon field leads to an increase or decrease of the inter-vehicular distance and in the worst case to collision (collision induction attack) [44]. Conversely, in replay attacks the adversary starts listening the messages wirelessly sent on networks, but, after storing the content of the message, it tries to retransmit the message at a later time. The attack effect can be very dangerous, leading eventually to vehicle's collision. Furthermore, it can be used to confuse the authorities and to hide the identification of the vehicles involved in an accident situation [109]. Differently, if an internal adversary vehicle forges the identities of multiple vehicles, the platoon is undergoing a Sybil attack. In this case, the false identities create the illusion that there exist additional vehicles along the road and this can be used to play any type of attack in the system [148]. Public key cryptography is a tool commonly proposed for dealing with these kind of attacks [4].
Considering now network layer attacks, in denial-of-service (DoS), an adversary overloads and overwhelms the communication capacity of a vehicle or of a group of vehicles by using vehicular botnets, in order to make them unable to exchange the necessary information for cooperative driving [67]. DoS attacks are considered very dangerous since they impact on the control algorithm correctly running, causing instability of the traffic flow and, in more severe cases, collisions. With respect to the

wide DoS category, note that during a burst attack the adversary tries to manipulate the data traffic flow in order to disperse only some beacons with a randomly loss rate distribution. In an eavesdropping attack, instead, the adversary extracts valuable information about the vehicles platoon and uses them for its own benefit. Furthermore, a platoon is said to be under a radio jamming attack when a deliberate communication disruption among platoon's members over small or wide geographic areas is implemented by using different techniques, such as one-channel jamming or several channels jamming. Malware attacks can also cause serious disruptions in normal VANETs operations. These attacks are normally executed by malicious insiders, rather than outsiders, whenever on board units (OBU) of vehicles and road side units (RSUs) perform software updates. The effect is an increase of transmission latency, which can be alleviated by using a centralized administration system[148]. Instead, during a black hole attack, a malicious vehicle declares having the shortest path to get the data and then it routes and redirects them. The adversary is hence able to intercept the data packet or retain it. When the forged route is successfully established, it depends on the malicious vehicle whether to drop or forward the packet [84]. Existing solutions to this attack consider designing protocols having more than one route to the destination, which imposes processing overload to the network [56]. As well as black hole, a wormhole is a severe attack. In this case two or more malicious vehicles create a tunnel to transmit data packets from one end of the network toward a malicious vehicle at the other end. By this way, these packets are broadcasted on the network and the malicious vehicles take the control of such a short network connection or link, hence threatening the security of transmitting data packets. To prevent wormhole attacks, packet leash is one of the most well known approaches (e.g. see [4] and references therein for more details). Another dangerous attack, referred in technical literature as byzantine [7], compromises either a single vehicle or a group of vehicles by creating routing loops and then directing data packets via non optimal paths, thus leading to degradation or disruption of the routing services [7]. To counteract this attack, the Robust Source Routing (RSR) protocol has been introduced, whose features allow delivering packets to their respective destinations even in Byzantine attack-like adversarial conditions [39]. Finally, a stealthy attack includes both side- and covert-channel exploitation (by

observing the traffic load in the physical level or hiding data flows within the regular messages) and passive traffic analysis (to learn from the network topology and/or deduce vehicles activity patterns, lifestyle and routes) [7].
Malicious attacks can also occur at system level. These are due to the tampering of vehicles hardware or software, that can be done both by a malicious insider at manufacturing level, and by an outsider in an unattended vehicle (for instance by replacing or altering certain vehicle sensors). In all these cases, if the on-board hardware/software is tampered with, or it is faulty, the input information to the system turn out to be not accurate, even if the communication channel is secure and an up-to-date architecture is implemented on the VANET. This lack of accuracy seriously affects the operation of the high-level protocols and, hence, the risk of tampering should be not neglected. To cope with this kind of attacks, the most popular solution presented in the technical literature is to use tamper-proof sensors [56]. Among the system level attacks, illusion attacks are particularly dangerous since the adversary purposefully deceives the sensors on his car in order to produce wrong sensor readings. This causes incorrect traffic warning messages that are broadcasted to neighbors. Hence, leveraging information from a cheating sensor, an attacker, who is an insider, can alter perceived position, speed, and direction of the other vehicles, thus inducing mishaps [84].
It is worth mentioning here that for the special case of electric vehicles, there exist specific security vulnerabilities, such as fraud and energy theft. To solve these problems, different solutions, devoted to improve the security of the Open Charge Point Protocol, have been proposed in the very recent technical literature (see [7] and references therein).
In this work, we consider self-contained vehicles equipped with internal combustion engines [11] and focus our attention on spoofing and message falsification, for the class of attacks at application layer, and on Denial of Service and Burst Transmission, for the class of attacks at network layer. As for the spoofing attack, we assume there is an internal opponent (i.e. a vehicle traveling inside the platoon) that imposes a constant offset at its current acceleration value from a given time instant. It then returns erroneous information to other vehicles within its communication range for disturbing their motion. For a message falsification attack, an internal opponent, who manipulates and falsifies the content of the

beacons to be sent to its neighbors, is considered. Specifically, it adds a constant offset value to its current position value such as to compromise the safe inter-vehicle distance. Furthermore, with respect to Denial of Service (DoS) attacks, we consider one external network intruder or one internal adversary that periodically overloads and overwhelms the communication capacity of one specific vehicle within the platoon. For the burst transmission attack (a particular type of DoS) it is instead assumed that one external network intruder, or one internal adversary, tries to manipulate the data traffic flow in order to disperse some beacons with a randomly loss rate. More details about the analyzed attacks are in Section 6.5.2.

6.2.2 Malicious Attack Countermeasures in Platooning Applications

Here, we discuss the main countermeasures for detecting and mitigating the malicious attacks presented above, in order to make the platooning application safer.
Cryptographic control method is one of the most useful tools [79, 159, 26, 5, 141, 201, 85, 121], especially if the opponent is an outsider. Indeed, the control system provides several services as authentication, data integrity and non repudiation [134], hence preventing vehicle impersonation or messages alteration. However when the adversary is an insider attacker, it possesses a valid recognition certificate. Thus the only use of cryptographic system control is not enough to solve cyber threats [222]. Moreover nonce technique [79], consisting in the use of an arbitrary number that may only be used once in the beacon message, can be useful in preventing the replay attacks.
Other effective solutions include reputation- and trust-based systems [204, 49, 52, 47]. Reputation is a widely used index for constructing the credibility of a vehicle within the network and Bayesian reputation functions are commonly used to calculate these reputation values. Leveraging reputation-based approaches, vehicles with a low confidence level are isolated from the others and they are eventually deprived from receiving any service [47]. Most of the approaches rely on the monitoring of neighboring vehicles, in order to evaluate their trustiness, or on a reputation management system (e.g. see [49] and references therein for further details). Also, Intrusion Detection Systems (IDSs) have shown

their efficiency in detecting with a high accuracy both internal and external attacks by using special agent-nodes that monitor both the behavior of target vehicles and the network traffic response. An alarm is triggered any time when a malicious behavior is detected [171]. Broadly intrusion detection techniques can be classified into the following categories [110]: signature-based detection methods, in which the intrusion detection system monitors the packets and matches them with existing signatures (e.g. see [137]); anomaly-based detection tools in which the system activities are monitored and, hence, declared as malicious or anomalous on the basis of some predefined rules rather than signatures (e.g. see [3, 171]); hybrid detection approaches in which the detection of malicious activities leverages either signature-based or anomaly-based methods (e.g. see [149]). Finally, note that, with the aim of improving detection performance, the IDSs are often endowed with computational intelligence. To this aim, neural networks, fuzzy rules, soft computing and machine leaning techniques are the most widely exploited tools in the field (e.g. see [175] and references therein).

With respect to the specific platoon application, the control strategy design plays an important role in providing further robustness and security and, hence, in enhancing the protection level of the normal operation of the autonomous driving process. Indeed, although the information security field has developed both advanced technologies and tools for preventing and reacting to attacks, embedding security in control design can be crucial, since an opponent, attacking the cyber infrastructure, can interfere the normal operation of physical process [75, 124].

A possible solution in this direction would consist in implementing a control algorithm allowing the detection of malfunctions and/or anomalies. Comparing the expected behavior of the vehicles platoon with the actually observed one, each vehicle would be able to detect a malicious information and to react adequately. This kind of approach has been for example considered in [44], where a model-based detection scheme is presented: each vehicle exploits wireless communication to model the expected behavior of its preceding vehicle; if the expected and actual behavior differ, the monitoring vehicle downgrades to non cooperative Adaptive Cruise Control (ACC), exploiting only radar measurement. Collaborative-decision technique, such as voting, could be also useful in detection and mitigation of malicious attacks. Note that, although the

idea of voting for detecting the malicious behavior has been proposed for years and several solution has been proposed to counteract the malicious attacks at network level [161, 202, 2, 71], no one exploits the technique at control level. Voting or fusion techniques can be effective tools for enhancing control security in platooning application. Indeed, by leveraging information redundancy (that is high especially in all-to-all or deeply connected configurations) it is possible to help the detection of some malicious behaviors [11, 151]. Furthermore in [13] another mitigation technique, embedded on-board vehicles platoon, is proposed: when a vehicle receives a message, before accepting the information, it checks the identification of the vehicle and the consistence of the message to avoid the acceptance of malicious information.

In [78] an example of wireless jamming attack is described. In this work the authors highlight how a correct control strategy design for the vehicles platoon, embedded with an estimator of the lost information, is able to mitigate the malicious effect of jamming. Finally, another mitigation technique is presented in [23], where a fuzzy algorithm for attack detection is proposed.

Hence, from literature overview, it is clear that the control strategy design plays an important role in robustness and security issues. Within this scenario, this chapter tackles and solves the platoon control problem in the presence of malicious attacks as a second order consensus problem, accounting for time varying communication delays and vehicles dynamics. Based on the effects of malicious attacks such as messages manipulation and communication capabilities impairments, we design a novel robust control strategy mixed to a voting technique for cooperative driving in an adversarial environment. The proposed control algorithm significantly enhances the state of art. Differently from [11], in which platoon instability arises for the presence of security vulnerabilities, the proposed robust strategy guarantees the platoon stability also in the presence of adversaries. Differently from [44], the mitigation technique implemented in this paper is able to react to malicious attacks without downgrading the cooperative strategy to the non cooperative ACC one. Finally, different from [78], we do not necessitate of an estimate of lost information since we design the strategy taking into account the eventual cyber attack on the vehicle communication capabilities. Furthermore we point out that

the control strategy overcomes the limitation of the V2V communication structure that is not restricted to the Predecessor-Follower one as assumed in [11, 44].

6.3 Collaborative Strategy for Platooning and Countermeasure for Malicious Behaviors

Our aim is to regulate the speed and the relative distance of each vehicle with respect to the neighboring vehicles in its communication range and to the leading vehicle, respectively [185, 38] in the presence of adversaries. The platoon is composed of N vehicles traveling on a single lane plus the additional leading vehicle acting as a reference for the ensemble. The adversary or the vehicle controlled by the adversary is part of the vehicles platoon and thus it is able to send valid V2V messages [124].
Since vehicles are moving within a non-ideal wireless communication environment, information can be received by each vehicle with different (often defined as multiple or heterogeneous) time-varying delays, whose current value is not random, but depends on the actual network conditions [30, 218]. Hence, in practice, communication impairments are unavoidable and therefore the control input, that is computed on the basis of outdated information, turns out to be affected by time-varying delays [164].
To model the generic i-th vehicle dynamics ($i = 1, \ldots, N$) we exploit the second-order longitudinal model in (3.3), i.e.

$$\begin{aligned} \dot{r}_i(t) &= v_i(t) \\ \dot{v}_i(t) &= \tfrac{1}{M_i} u_i(t), \end{aligned} \tag{6.1}$$

where r_i [m] and v_i [m/s] are the i-th vehicle absolute position (with respect to a given reference framework) and speed; M_i [kg] is the i-th vehicle mass and the propelling force u_i denotes the control input to be appropriately chosen to achieve the control goal.
Similarly, the leader vehicle dynamics are

$$\begin{aligned} \dot{r}_0(t) &= v_0 \\ \dot{v}_0 &= 0 \end{aligned} \tag{6.2}$$

being r_0 and v_0 the leader state variables.
Given (6.1) and (6.2), the problem of maintaining a desired inter-vehicle

spacing policy and a common constant speed (as imposed by the leader) can be rewritten as the following second-order consensus problem

$$\begin{aligned} r_i(t) &\to \tfrac{1}{\Delta_i}\left\{\textstyle\sum_{j=0}^{N} \alpha_{ij}\cdot(r_j(t)+s_{ij})\right\} \\ v_i(t) &\to v_0, \end{aligned} \tag{6.3}$$

where s_{ij} is the desired distance between vehicles i and j; α_{ij} (for $i = 1,...,N$ and $j = 0,...,N$) models the platoon communication topology emerging from the presence/absence of a communication link between vehicles i and j; Δ_i is the degree of vehicle i, i.e. the number of vehicles establishing a communication link with vehicle i.
According to [41], the desired spacing s_{ij} can be expressed as $s_{ij} = h_{ij}v_0 + s_{ij}^{st}$, where h_{ij} is the headway time and s_{ij}^{st} is the distance between the vehicles i-th and j-th at standstill. Furthermore we remark that α_{ij} are the non negative elements of the adjacency matrix associated to the platoon topology directed graph $\mathcal{G}_{N+1}$.
The platoon goal in (6.3) is here achieved by using a distributed strategy that explicitly counteracts the presence of communication impairments, such as time-varying delays (e.g. due to packet losses, that affect each communication link at a given time instant t) and that embeds a local detection of compromised communication information, that are hence discarded for the trust computation of the control protocol. To this aim, each vehicle in the platoon checks, at each time step, for anomalies in the data wirelessly received from the members of the group with a collaborative decision-making technique (voting techinque) that enables vehicles to collectively shield themselves against a misbehaving vehicle. Note that, monitoring solutions, with the aim of excluding in a real-time mode a faulty node for preserving quality in wireless sensor networks, often leverage a generic neighborhood voting with a decentralized approach and adopt in practice a comparison with some threshold value that is usually related to the distance from an average desired behavior (see [142, 33] and references therein). In the specific case of a platoon application, we implement a similar approach by computing the average distance between vehicles in nominal conditions. This average value is locally computed by each vehicle at the engagement of the platoon during the initialization step of the voting algorithm.
The control input to each vehicle, on board computed on the basis of

trusted information obtained by the voting procedure, is hence chosen as

$$u_i(t) = -b\,[v_i(t) - v_0] - \tfrac{1}{\Delta_i} \sum_{\substack{j=0 \\ j \notin \mathcal{M}}}^{N} k_{ij}\alpha_{ij}[d_{ij}(t) - \tau_{ij}(t)v_0], \qquad (6.4)$$

where $d_{ij}(t) = r_i(t) - r_j(t - \tau_{ij}(t)) - s_{ij}$ is the actual inter-vehicle distance between vehicle i and vehicle j on-board computed from transmitted data according to the required spacing policy; k_{ij} and b are control gains to be opportunely tuned to regulate the mutual behavior among neighbor vehicles; $\tau_{ij}(t)$ is the time-varying communication delays affecting the i-th vehicle when information are transmitted from its neighbor j. The delays $\tau_{ij}(t)$ are bounded [167, 25, 101, 102] and detectable through the time stamp embedded in transmitted information [167, 32]. Moreover $\mathcal{M} = \{m_1, m_2, \cdots, m_\rho\}$ (with $\rho \leq N$) is the set of detected malicious vehicles, or nodes.

In order to update the set of malicious node $\mathcal{M}$, each vehicle i of the platoon, during traveling, collects all information, sent by all the other vehicles in its communication range and shared via V2V. We further remark that we consider that the vehicles platoon is formed and it is traveling at its steady-state with a prescribed spacing policy and with a constant velocity.

Data are locally exploited for constructing, according to the control protocol in (6.4), a 'belief' about the average distance under the ideal assumption that all information are correct (e.g. $\mathcal{M} = \emptyset$) and defined as

$$\bar{d}_i(t) = \frac{1}{\Delta_i} \sum_{j=0}^{N} \alpha_{ij}\,[r_i(t) - r_j(t - \tau_{ij}(t)) - s_{ij} - \tau_{ij}(t)v_0]\,. \qquad (6.5)$$

This average value $\bar{d}_i(t)$ is compared with the actual inter-vehicular distance between vehicle i and vehicle j ($\forall j = 1, \cdots, N$, $j \neq i$) defined as

$$\gamma_{ij}(t) = [d_{ij}(t) - \tau_{ij}(t)v_0]\,. \qquad (6.6)$$

If there is a significant discrepancy in the belief, i.e. if, for a certain vehicle this difference is grater than a threshold δ, it might be an indicator of a security compromise in the communication channel and hence information coming from the malicious vehicle are not exploited for the longitudinal control of vehicle i and the set $\mathcal{M}$, that enumerates the malicious nodes,

Algorithm 1: Safe distributed control strategy pseudo-code for the i-th vehicle

Data: v_0, $r_j(t)$ and $\tau_{ij}(t)$ $(\forall\, j = 0, 1, \cdots, N)$
Result: The control effort $u_i(t)$
Declarations

$$d_{ij}(t) = r_i(t) - r_j(t - \tau_{ij}(t)) - s_{ij};$$

$$\bar{d}_i(t) = \frac{1}{\Delta_i} \sum_{j=0}^{N} a_{ij} \left[d_{ij}(t) - \tau_{ij}(t) v_0 \right];$$

$$\gamma_{ij}(t) = \left[d_{ij}(t) - \tau_{ij}(t) v_0 \right].$$

Initialization (platoon engaged)

$$\mathcal{M} = \emptyset;$$

$$\rho = 1;$$

$$\delta = 0.5;$$

$$\Delta_i = \sum_{j=0}^{N} a_{ij};$$

$$s_{ij} = h_{ij} v_0(0) + s_{ij}^{st}.$$

for $j = 1$ **to** N **do**
  if $\epsilon_{i,j}(t) = \|\bar{d}_i(t) - \gamma_{ij}(t)\| > \delta$ **then**
    Detection of malicious vehicle j:

$$m_\rho = j;$$

$$\rho = \rho + 1;$$

    Updating of the set of detected malicious vehicles:

$$\mathcal{M} = \mathcal{M} \cup \{m_\rho\}$$

  end

$$u_i(t) = -b \left[v_i(t) - v_0 \right] - \frac{1}{\Delta_i} \sum_{\substack{j=0 \\ j \notin \mathcal{M}}}^{N} k_{ij} \alpha_{ij} \gamma_{ij}(t);$$

end

is updated accordingly. The procedure is repeated for all vehicles within the platoon at each time step.

A schematic overview of the functioning of the safe distributed control strategy is reported in Algorithm 1. Note that, as usual, the information received by the leading vehicle, i.e. the reference behavior for platoon, is

not falsified (for example assuming the usage of cryptographic security procedures in terms of digital signatures [124]) while all information transmitted by the other vehicles within the platoon can be compromised. We finally remark that the proposed approach is flexible since it fits different communication topologies in which the leading vehicle is globally reachable (see Figure 3.5 for different examples). Alternative attempts are instead designed with respect to a pre-fixed communication structure, e.g. predecessor-follower as in [11].

6.4 Stability Analysis

6.4.1 Vehicular Network Dynamics

To derive the platoon dynamics under the action of the collaborative strategy in (6.4), and then prove its convergence, we first define the position and speed errors with respect to the reference signal $r_0(t)$, v_0 $(i = 1, \ldots, N)$ as

$$\begin{array}{l} \bar{r}_i(t) = r_i(t) - r_0(t) - h_{i0}v_0 - s_{i0}^{st} \\ \bar{v}_i(t) = v_i(t) - v_0. \end{array} \tag{6.7}$$

Re-writing the control action $u_i(t)$ (see (6.4)) in terms of the state error (see (6.7)), expressing h_{ij} and the standstill distance s_{ij}^{st} with respect to the leading vehicle (namely $h_{ij} = h_{i0} - h_{j0}$ and $s_{ij}^{st} = s_{i0}^{st} - s_{j0}^{st}$), the closed-loop dynamics can be rewritten $\forall i = 1, \ldots, N$ as

$$\left\{ \begin{array}{ll} \dot{\bar{r}}_i = \bar{v}_i & \\ M_i\dot{\bar{v}}_i = & -b\bar{v}_i - \frac{1}{\Delta_i}(k_{i0}\alpha_{i0} + \sum_{j=1}^{N} k_{ij}\alpha_{ij})\bar{r}_i(t) \\ & +\frac{1}{\Delta_i}\sum_{j=1}^{N} k_{ij}\alpha_{ij}\bar{r}_j(t - \tau_{ij}(t)). \end{array} \right. \tag{6.8}$$

To describe the platoon dynamics in the presence of cyber threats and time-varying delays, associated to the different links, in a more compact form, we define the position and the speed errors vectors as $\bar{r}(t) = \left[\bar{r}_1^\top(t) \cdots \bar{r}_i^\top(t) \cdots \bar{r}_N^\top(t) \right]^\top \in \mathbb{R}^N$, $\bar{v}(t) = \left[\bar{v}_1^\top(t) \cdots \bar{v}_i^\top(t) \cdots \bar{v}_N^\top(t) \right]^\top \in \mathbb{R}^N$, and the error state vector as $\bar{x}(t) = \left[\bar{r}^\top(t) \ \bar{v}^\top(t) \right]^\top \in \mathbb{R}^{2N}$. Furthermore, delays $\tau_{ij}(t)$ can be represented as elements of the following delay set: $\tau_p(t) \in \{\tau_{ij}(t) : i, j =$

$1, 2, ..., N, i \neq j\}$ for $p = 1, 2, ..., m$ with $m \leq N(N-1)$. Note that m is equal to its maximum value if the underlying network topology is a directed complete graph and all time-delays are different.
According to the above definition, the closed-loop platoon dynamics can be represented as the following set of functional differential equations:

$$\dot{\bar{x}}(t) = A_0 \bar{x}(t) + \sum_{p=1}^{m} A_p \left(\bar{x}(t - \tau_p(t))\right), \tag{6.9}$$

where

$$A_0 = \begin{bmatrix} 0_{N\times N} & I_{N\times N} \\ -M\widetilde{K} & -M\widetilde{B} \end{bmatrix} \in \mathbb{R}^{2N\times 2N}, \tag{6.10}$$

$$A_p = \begin{bmatrix} 0_{N\times N} & 0_{N\times N} \\ M\widetilde{K}_p & 0_{N\times N} \end{bmatrix} \in \mathbb{R}^{2N\times 2N}, \tag{6.11}$$

being

$$M = diag\Big\{\frac{1}{M_1}, \cdots, \frac{1}{M_N}\Big\} \in \mathbb{R}^{N\times N}; \tag{6.12}$$

$$\widetilde{B} = diag\Big\{b, \cdots, b\Big\} \in \mathbb{R}^{N\times N}; \tag{6.13}$$

$$\widetilde{K} = diag\Big\{\widetilde{k}_{11}, \cdots, \widetilde{k}_{NN}\Big\} \in \mathbb{R}^{N\times N}, \quad \text{with } \widetilde{k}_{ii} = \tfrac{1}{\Delta_i}\sum_{j=0}^{N} k_{ij}\alpha_{ij}; \tag{6.14}$$

and $\widetilde{K}_p = [\widetilde{k}_{pij}]$ is the matrix defined as:

$$\widetilde{k}_{pij} = \begin{cases} \frac{\alpha_{ij}k_{ij}}{\Delta_i}, & j \neq i,\ \tau_p(\cdot) = \tau_{ij}(\cdot)\,, \\ 0, & j \neq i\,, \tau_p(\cdot) \neq \tau_{ij}(\cdot)\,, \\ 0, & j = i\,. \end{cases} \tag{6.15}$$

6.4.2 Proof of Convergence

In this section we analytically prove the convergence of the proposed approach. The stability analysis is based on the recast of the closed-loop dynamics as a set of functional differential equations for which it is

possible to find a quadratic Lyapunov-Krasovskii function [73, 62].
From Leibniz-Newton (see Definition 4) it is known that [184]

$$\bar{x}(t-\tau_p(t)) = \bar{x}(t) - \int_{-\tau_p(t)}^{0} \dot{\bar{x}}(t+s)ds \ . \tag{6.16}$$

Hence substituting (6.9) in (6.16) we have:

$$\bar{x}(t-\tau_p(t)) = \bar{x}(t) - \sum_{q=0}^{m} A_q \int_{-\tau_p(t)}^{0} \bar{x}(t+s-\tau_q(t+s))ds \ , \tag{6.17}$$

where matrices $A_0,\ A_1,\ \ldots,\ A_m$ are defined in (6.10), (6.11) and $\tau_0(t+s)=0$. Using the above transformation, the time-delayed model (6.9) can be transformed into

$$\begin{array}{rl} \dot{\bar{x}}(t) & = A_0\bar{x}(t) + \sum_{p=1}^{m} A_p\bar{x}(t) + \\ & - \sum_{p=1}^{m}\sum_{q=0}^{m} A_pA_q \int_{-\tau_p(t)}^{0} \bar{x}(t+s-\tau_q(t+s))ds \ . \end{array} \tag{6.18}$$

From the definition in (6.10) and in (6.11), it follows that $A_pA_q = 0$ when $p = 1,\ldots,m$ and $q = 1,\ldots,m$. Hence the system defined in (6.9) can be written as

$$\dot{\bar{x}}(t) = F\bar{x}(t) - \sum_{p=1}^{m} C_p \int_{-\tau_p(t)}^{0} \bar{x}(t+s)ds, \tag{6.19}$$

where

$$C_p = A_pA_0 = \begin{bmatrix} 0_{N\times N} & 0_{N\times N} \\ 0_{N\times N} & M\widetilde{K}_p \end{bmatrix}, \tag{6.20}$$

and

$$F = A_0 + \sum_{p=1}^{m} A_p = \begin{bmatrix} 0_{N\times N} & I_{N\times N} \\ -M\widehat{K} & -M\widetilde{B} \end{bmatrix}, \tag{6.21}$$

with

$$\widehat{K} = -\sum_{p=1}^{m} \widetilde{K}_p + \widetilde{K}. \tag{6.22}$$

Furthermore the following lemmas hold:

Lemma 5. *[167] Supposing $k_i = \frac{k_{i0}\alpha_{i0}}{\Delta_i} \geq 0$ $(i = 1,\ \ldots,\ N)$, the matrix $\widehat{K}$ in (6.22) is positive stable (see definition in [55]) if and only if node 0 is globally reachable in $\mathcal{G}_{N+1}$.*

According to Lemma 5 the following matrix

$$\widehat{K}_M = M\widehat{K} \tag{6.23}$$

is also positive stable since $M > 0$ (Equation 6.12).

Lemma 6. *[167] Let F be the matrix defined in (6.21). F is Hurwitz stable if and only if $\widehat{K}_M$ (6.23) in Lemma 5 is positive stable and*

$$b > \max_i \left\{ \frac{|Im(\mu_i)|}{\sqrt{Re(\mu_i)}} M_i \right\} \tag{6.24}$$

being μ_i the i-th eigenvalue of $\widehat{K}_M$ ($i = 1, \ldots, N$).

Stability in the presence of the heterogeneous time-varying delays can be now guaranteed under the classical constraints on bounded delay functions [73], i.e $\tau_p(t) \in [0;\ \tau_p^\star]$, $\dot{\tau}_p(t) \in [0, d_p] \quad \forall t,\ \forall p$ and $d_p \leq 1$, according to the following LMI-based criterion that can be easily verified by using, for example, the interior-point method [27] implemented in the Yalmip © Toolbox [128].

Theorem 7. *Consider the vehicular network in (6.9) under the assumptions of Lemma 5 and Lemma 6. Also assume all delays $\tau_p(t)$ ($p = 1, \ldots, m$) to be bounded. If there exist constant, symmetric and positive definite matrices $P \in \mathcal{R}^{2N\times 2N}$ and $S_p \in \mathcal{R}^{2N\times 2N}$ ($p = 1, \ldots, m$) such that it holds*

$$\begin{cases} \frac{\tau^\star}{2} P - S_1(1 - d_1) < 0 \\ \qquad \vdots \\ \frac{\tau^\star}{2} P - S_m(1 - d_m) < 0\ , \end{cases} \tag{6.25}$$

then the closed loop system (6.9) is asymptotically stable, i.e.

$$\lim_{t\to\infty} x(t) = 0 \tag{6.26}$$

for

$$\tau^\star = \max_p \{\tau_p^\star\} < \frac{\|Q - \sum_{p=1}^m S_p\|}{\|\sum_{p=1}^m PC_pP^{-1}C_p^\top P^\top + \frac{P}{2}\|}\ . \tag{6.27}$$

Proof. Consider the following Lyapunov-Krasovskii function for system in (6.19):

$$V(\bar{x}(t)) = \bar{x}^\top(t)P\bar{x}(t) + \sum_{p=1}^m \int_{t-\tau_p(t)}^t \bar{x}^\top(s)S_p\bar{x}(s)ds, \tag{6.28}$$

where $P = P^\top > 0 \in \mathbb{R}^{2N\times 2N}$ and $S_p > 0 \in \mathbb{R}^{2N\times 2N}$ $(p = 1, \ldots, m)$ are appropriately chosen. According to the hypothesis of Lyapunov-Krasovskii theorem [73], we define the following positive continuous non-decreasing functions

$$\begin{aligned} u(\bar{x}(t)) &= \bar{x}^\top(t)P\bar{x}(t) \\ v(\bar{x}(t-\tau^\star)) &= \bar{x}^\top(t)P\bar{x}(t) + \sum_{p=1}^{m} \int_{t-\tau^\star}^{t} \bar{x}^\top(s)S_p\bar{x}(s)\,ds, \end{aligned} \tag{6.29}$$

with $\tau^\star = \max_p\{\tau_p^\star\}$ such that

$$u(\bar{x}(t)) \leq V(\bar{x}(t)) \leq v(\bar{x}(t-\tau^\star)). \tag{6.30}$$

Now differentiating the functional in (6.28) along the trajectories of the system (6.19) it follows

$$\begin{aligned} \dot{V}(\bar{x}(t)) = \; & \bar{x}^\top(t)\left(PF + F^\top P + \textstyle\sum_{p=1}^{m} S_p\right)\bar{x}(t) \\ & -2\bar{x}(t)P\textstyle\sum_{p=1}^{m} C_p \int_{-\tau_p(t)}^{0} \bar{x}^\top(t+s)\,ds \\ & -\textstyle\sum_{p=1}^{m} \bar{x}^\top(t-\tau_p(t))S_p\bar{x}(t-\tau_p(t))(1-\dot{\tau}_p)\,. \end{aligned} \tag{6.31}$$

By selecting the control gains k_{ij}, b according to Lemma 5, Lemma 6 and by considering the global reachability for the leading vehicle, it follows that the matrix F in (6.21) is Hurwitz stable (see definition in [55]). Thus, according to the Lyapunov theory (see [104]) we have $PF + F^\top P = -Q$ with $Q > 0 \in \mathbb{R}^{2N\times 2N}$.
Furthermore, by exploiting Lemma 3 in which we set $a = -\bar{x}^\top(t)PC_p$, $c = \bar{x}(t+s)$, $\Xi = P^{-1}$ and integrating both side of the inequality, equation (6.31) becomes

$$\begin{aligned} \dot{V}(\bar{x}(t)) \; & \leq -\bar{x}^\top(t)Q\bar{x}(t) + \bar{x}^\top(t)\textstyle\sum_{p=1}^{m} S_p\bar{x}(t) \\ & + \textstyle\sum_{p=1}^{m}\left[\tau_p(t)\bar{x}^\top(t)PC_pP^{-1}C_p^\top P^\top\bar{x}(t) + \int_{-\tau_p(t)}^{0} \bar{x}^\top(t+s)\,ds\right] \\ & - \textstyle\sum_{p=1}^{m} \bar{x}^\top(t-\tau_p(t))S_p\bar{x}(t-\tau_p(t))(1-\dot{\tau}_p)\,. \end{aligned} \tag{6.32}$$

Now, applying Jensen Inequality (see Lemma 2) to the integral terms and exploiting the bound on the delay function [63], inequality (6.32)

can be recast as

$$\begin{aligned}\dot{V}(\bar{x}(t)) \leq \; & -\bar{x}^\top(t)Q\bar{x}(t) + \bar{x}^\top(t)\textstyle\sum_{p=1}^{m} S_p\bar{x}(t) \\ & + \textstyle\sum_{p=1}^{m}\big[\tau^\star\bar{x}^\top(t)PC_pP^{-1}C_p^\top P^\top\bar{x}(t) \\ & + \frac{\tau^\star}{2}\left(\bar{x}^\top(t)P\bar{x}(t) + \bar{x}^\top(t-\tau_p(t))P\bar{x}(t-\tau_p(t))\right)\big] \\ & - \textstyle\sum_{p=1}^{m}\bar{x}^\top(t-\tau_p(t))S_p\bar{x}(t-\tau_p(t))(1-d_p)\;.\end{aligned} \tag{6.33}$$

Now, by defining an augmented state error vector $\zeta(t) = [\bar{x}(t),\ \bar{x}(t-\tau_1(t)),\ \cdots,\ \bar{x}(t-\tau_m(t))] \in \mathbb{R}^\rho$, with $\rho = (m+1)2N$, it is possible to re-write (6.33) in a more compact form as

$$\dot{V}(\bar{x}(t)) \leq \zeta^\top(t)\Theta\zeta(t)\;, \tag{6.34}$$

where $\Theta \in \mathbb{R}^{\rho\times\rho}$ is the following diagonal blocks matrix:

$$\Theta = \begin{bmatrix} \theta_{1,1} & 0_{2N\times 2N} & \cdots & \cdots & 0_{2N\times 2N} \\ 0_{2N\times 2N} & \theta_{2,2} & 0_{2N\times 2N} & \vdots & \vdots \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ \vdots & \ddots & 0_{2N\times 2N} & \theta_{m,m} & 0_{2N\times 2N} \\ 0_{2N\times 2N} & \cdots & \cdots & 0_{2N\times 2N} & \theta_{m+1,m+1} \end{bmatrix}, \tag{6.35}$$

with

$$\begin{aligned} &\theta_{1,1} = -Q + \textstyle\sum_{p=1}^{m} S_p + \sum_{p=1}^{m}\frac{\tau^\star}{2}\left[2PC_pP^{-1}C_p^\top P^\top + P\right], \\ &\theta_{2,2} = \tfrac{\tau^\star}{2}P - S_1(1-d_1), \\ &\vdots \\ &\theta_{m+1,m+1} = \tfrac{\tau^\star}{2}P - S_m(1-d_m). \end{aligned} \tag{6.36}$$

Now, from (6.34) stability can be proved by showing $\dot{V}(\bar{x}(t)) \leq 0$. Given (6.35), to this aim we have to show that each diagonal blocks has to be negative definite, i.e.

$$-Q + \sum_{p=1}^{m} S_p + \sum_{p=1}^{m}\frac{\tau^\star}{2}\left[2PC_pP^{-1}C_p^\top P^\top + P\right] < 0 \tag{6.37}$$

and

$$\begin{cases} \frac{\tau^\star}{2}P - S_1(1-d_1) < 0 \\ \vdots \\ \frac{\tau^\star}{2}P - S_m(1-d_m) < 0\;. \end{cases} \tag{6.38}$$

Since $d_p < 1 \; \forall p$, from the hypothesis of the theorem in (6.25) it follows that the LMI problem in (6.37) and (6.38) can be solved by selecting the delay bound $\tau^\star$ as (6.27). Furthermore, given the choice made for $u(\bar{x}(t))$ in (6.29), the closed-loop vehicular network in (6.9) is also globally asymptotically stable according to Lyapunov-Krasovskii theorem [73]. This completes the proof. □

Remark 4. *We remark that Algorithm 1 is embedded into the control protocol and hence it has to be meant as an integral part of it. In so doing, its correctness proof is provided through the above analytical derivation where the convergence of the whole control protocol is proven by using a Lyapunov-Krasovskii approach.*

6.5 Numerical Analysis

6.5.1 Network and Traffic Scenario

To show the effectiveness of the proposed strategy for cooperative driving in the presence of malicious attacks (detailed in the following Section 6.5.2), here we consider a 10 $[km]$ freeway where an automated platoon of seven vehicles plus the leader, connected via the IEEE 802.11p communication protocol, travels along a single lane. To validate the theoretical results the collaborative strategy presented in section 6.3 is implemented in PLEXE[172].

The exemplar analysis has been carried out for two representative driving maneuvers, namely: (i) maintaining tight formation - starting from different initial conditions, the platoon has to reach and maintain the reference behavior as imposed by the leader, that moves with a constant velocity, while it achieves at the same time the desired spacing policy [167]; (ii) leader tracking - all followers have to correctly track the time-varying leader speed.

Furthermore, with the aim of disclosing the flexibility of the approach with respect to information flows, the investigation is conducted for the different communication topologies depicted in Fig. 3.5, that are the most frequently used for platoon applications [59]. Table 7.1 and Table 8.1 summarize all relevant parameters for both network and traffic simulation. Note that the value of the theoretical delay margin computed as in (6.27) and reported in Table 8.1, $\tau^\star = 0.18$ $[s]$, is within the average end-to-end

Table 6.1: NETWORK SIMULATION PARAMETERS.

Realistic channel	
Path loss model	Free space ($\alpha = 2.0$)
Fading model	Nakagami-m ($m = 3$)
PHY/MAC model	IEEE 802.11p/1609.4 single channel (CCH)
Frequency	5.89 $[GHz]$
Bitrate	6 $[Mbits^{-1}]$ (QPSK R = $\frac{1}{2}$)
Access category	AC_VI
MSDU size	200 $[B(byte)]$
Transmit power	20 $[dBm]$
Beacon frequency	10 $[Hz]$

Table 6.2: TRAFFIC SIMULATION PARAMETERS.

Freeway length	10 $[km]$
Lanes	4 (two-way)
Cars speed	100 $[Kmh^{-1}]$
Platoon size	8 cars
Platooning car max acceleration	3.5 $[ms^{-2}]$
Platooning car mass	1460 $[Kg]$
Platooning car length l_i	4 $[m]$
Headway time h_{ij}	0.8 $[s]$
Control gains k_{ij}	$k_{10} = 460$, $k_{i0} = 80$ $(i = 1, \cdots, N)$ $k_{i,i-1} = 860$, $k_{ij} = 0$ otherwise
Control gains b	$b = 1800$
Distance at standstill s_{ij}^{st}	15 $[m]$
Theoretical delay margin $\tau^{\star}$	0.18 $[s]$
Freeway fill-up time	500 $[s]$
Network warm-up time	10 $[s]$
Data recording time	50 $[s]$

communication delay, typical of IEEE 802.11p vehicular networks, which is of the order of hundredths of a second (i.e. $10^{-2}[s]$) [6]. This confirms a certain margin of stability robustness in practical working conditions. We remark that if the estimated theoretical bound was under the average value exhibited by the communication channel, robust stability could not be analytically guaranteed in all the network working conditions.

6.5.2 Description of the Attacks

In what follows we describe and consider the typical attacks that have been indicated as the main causes of vulnerability in cooperative driving applications, according to the very recent literature in the field of V2V connected vehicles (e.g. see [11]), i.e. Spoofing, Message Falsification, Denial of Service (DoS) and Burst Transmission.

6.5.2.1 Spoofing

In this kind of attack, an adversary impersonates a vehicle in the stream with the intention of injecting fraudulent information into a specific vehicle or of taking the control of the vehicle itself [24]. This kind of attack compromises the platoon maintenance and, in the worst case, it may cause collisions.
In our scenario we assume that an internal adversary (cryptography security procedures in terms of digital signatures are implemented to prevent external attacks [134]) takes the control of the third vehicle and imposes a constant offset to its current acceleration value, namely equal to 3.5 $[ms^{-2}]$ from a given time instant t. This implies that the third vehicle starts to improperly accelerate, then it incorrectly moves from the prescribed velocity and, hence, it perturbs the motion of all the vehicles within its communication range. The attack has to be mitigated by algorithms able to discard the incorrect information.

6.5.2.2 Message Falsification

An adversary, internal or external to the platoon, starts listening to the wireless messages exchanged among vehicles and, after receiving each beacon, it falsifies the content of messages. Finally, it rebroadcasts the malicious messages [44]. Countermeasures to this kind of attack rely on efficient detection algorithms, such as the voting technique presented in this paper, to construct a more well formed belief, which can then be checked against the vehicle belief. As well as spoofing, note that here we consider an insider malicious attacker since, if the adversary is external to the platoon, then cryptography security procedures would guarantee the prevention of the attack.
Specifically, in our exemplar analysis the adversary is the fourth vehicle of the fleet and it manipulates the position field of the beacon to be

sent by adding, at a specific time instant t, a value of $+5$ $[m]$ to its current position value. The incorrect information are then rebroadcast to the other vehicles. Note that, since passengers security is one of the most important issue for the platooning application diffusion, this kind of attack is very dangerous because it compromises the inter-vehicular distance and, in the worst case, it causes a collision.

6.5.2.3 Denial of Service

This attack aims to compromise the communication capability of a specific vehicle, or of a group of vehicles within the platoon, by making them unable to properly collaborate.
Specifically, here we consider that the third vehicle is under the DoS attack and it gets only the 70% of the exchanged information among vehicles within the platoon from a given time instant t. This lack of information downgrades the ability to correctly collaborate during driving and, thus, the attached vehicle may even collide with its predecessor. Possible countermeasures are based on the explicit compensation of the communication impairments. Note that the effects of a DoS attack are usually mitigated by technical solutions that act on the communication layer, such as channel switching, technology switching, frequency hopping, or multiple radio transceivers [11], [23, 85]. Hence, in our simulation scenario we suppose that the duration of each DoS attack is limited to a specific time interval, after which it is rejected. The DoS attack is then repeated again and again in a periodic fashion every 25 seconds (with a DoS time duration of 20 $[s]$ and with a percentage loss rate equal to 30%).

6.5.2.4 Burst Transmission

The burst transmission is a particular network attack that induces packet losses with a random loss rate. An internal or external adversary, at a specific time instant t, manipulates the data traffic flow in order to disperse some of the packets exchanged among vehicles. In particular here we consider a loss rate that randomly varies between 40% and 60%. The effect of this kind of attack can be disastrous, bringing vehicles platoon to collision. Note that both the DoS and the Burst Transmission require that the collaborative algorithms, robust with respect to

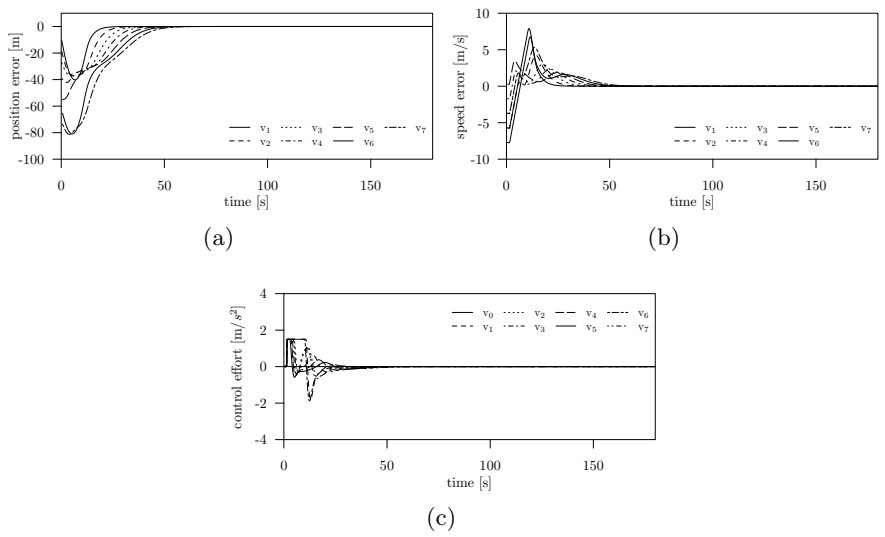


Figure 6.1: Maintaining tight formation maneuver under L-P-F topology: (a): time history of the position error computed as $r_i(t) - r_0(t) - d_{i0}$ ($\forall i = 1, \cdots, 7$); (b): time history of the speed error computed as $v_i(t) - v_0$ ($\forall i = 1, \cdots, 7$); (c): time history of the control effort $a_i(t)$ ($\forall i = 0, \cdots, 7$).

networks delays due to packet losses, are implemented together with cryptography solutions and authentication procedures for the access to vehicular networks [85].

6.5.3 Simulation Results

6.5.3.1 Platoon Condition without Attacks

To better understand and evaluate the impact of malicious attacks and the effectiveness of the collaborative strategy in counteracting misleading information, we show at first the ability of the approach in ideal conditions, when no adversary is present. As depicted in Figure 6.1, all vehicles, starting from distances different from the ones required by the spacing policy, converge toward the desired positions and the leader speed after about 60 seconds. This exemplar result refers to the classical L-P-F

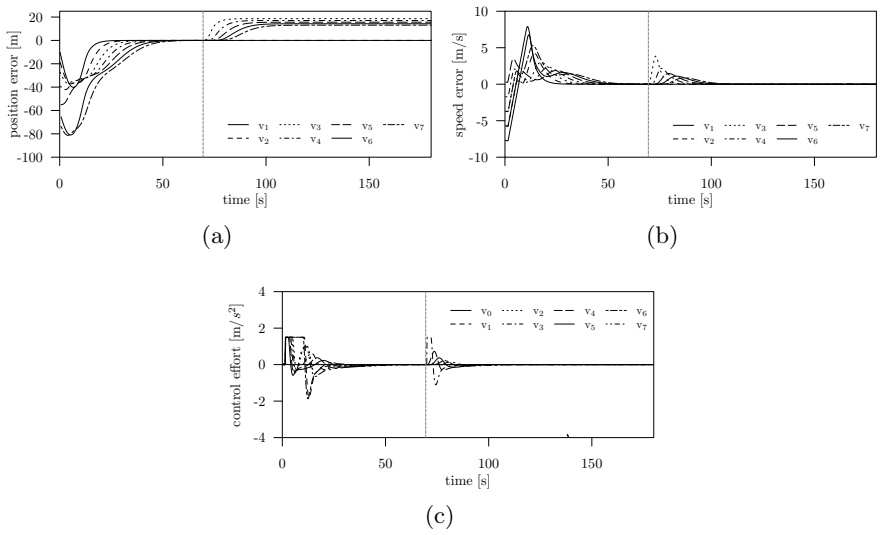


Figure 6.2: Effects of spoofing attack in nominal conditions (the malicious attack begins at time $t = 70$ $[s]$ as highlighted by the vertical gray dash line). Maintaining tight formation maneuver under L-P-F topology: (a): time history of the position error computed as $r_i(t) - r_0(t) - d_{i0}$ $(\forall i = 1, \cdots, 7)$; (b): time history of the speed error computed as $v_i(t) - v_0$ $(\forall i = 1, \cdots, 7)$; (c): time history of the control effort $a_i(t)$ $(\forall i = 0, \cdots, 7)$.

communication topology. Similar results can be achieved for alternative information flows, but they are omitted here for the sake of brevity.

6.5.3.2 Platoon Condition with Attacks

In what follows we present results with respect to the different attacks described in Section 6.5.2.

Spoofing Let consider the case of maintaining tight formation under a L-P-F communication topology. At $t = 70$ $[s]$, an internal adversary takes the control of the third vehicle and injects fraudulent information by setting its acceleration to the maximum value (see details in Section 6.5.2.1). To quantitatively investigate the effect of this spoofing

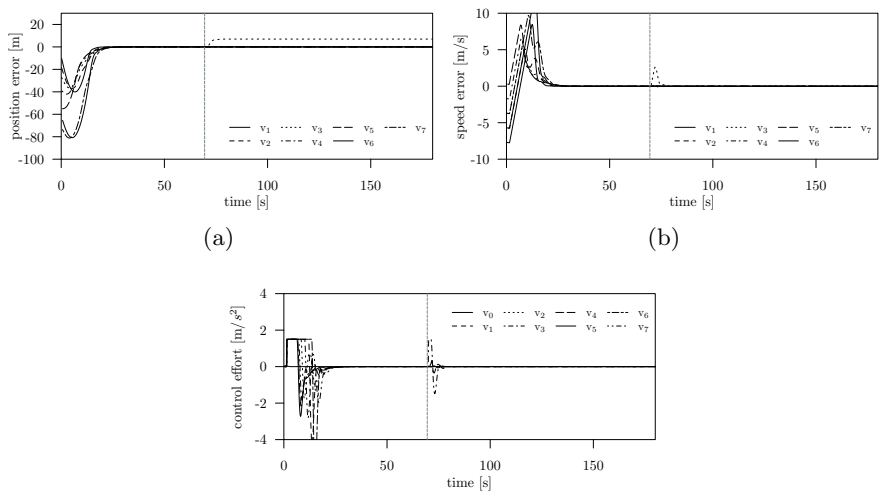


Figure 6.3: Spoofing attack (the malicious attack begins at time $t = 70$ $[s]$ as highlighted by the vertical gray dash line). Maintaining tight formation maneuver under L-P-F topology: (a): time history of the position error computed as $r_i(t) - r_0(t) - d_{i0}$ $(\forall i = 1, \cdots, 7)$; (b): time history of the speed error computed as $v_i(t) - v_0$ $(\forall i = 1, \cdots, 7)$; (c): time history of the control effort $a_i(t)$ $(\forall i = 0, \cdots, 7)$.

attack and to better disclose the ability of the collaborative strategy in counteracting its presence, we start presenting the platoon behavior in the case when the voting algorithm (Algorithm 1) is inactive and, hence, vehicles trust all information ($\mathcal{M} = \emptyset$ in (6.4) $\forall i$). Results in Figure 6.2 show how the spoofing strongly affects the correct inter-vehicular spacing policy (position error of vehicles $3 - 4 - 5 - 6 - 7$ does not converge to zero as highlighted in Figure 6.2a) while, after a brief transient of 30 $[s]$, the strategy is able to recover the velocity requirements (see Figure 6.2b and Figure 6.2c). The same dynamic behavior arises for P-F, B-L-F, and BR network topologies and hence it is omitted.
When enabling voting within the control protocol (i.e. Algorithm 1 is on), vehicles $4 - 5 - 6 - 7$ are instead able to discard the information falsified from vehicle 3 as shown in Figure 6.3 and, hence, they always satisfy the

spacing policy requirements (position errors go to zero, see Figure 6.3a). As expected, only for the third vehicle the effect of malicious is mitigated, but it is not completely rejected, since it is exposed to a direct attack on its acceleration signal. Nevertheless, collision avoidance is always ensured. The algorithm reacts to the cyber threat between 0.019 $[s]$ and 0.021] $[s]$. It reacts much faster than a human driver since the average human reaction time has been estimated to be approximately equal to 0.4 $[s]$ (e.g. see [206] and references therein for a technical discussion on the topic).

Similar good performance has been also noted for B-L-F and BR network topologies and results are hence omitted. A special remark has to be done for P-F topology. Here, due to the lack of information redundancy resulting from the very simple topology, the voting technique only working on V2V transmitted data can not be used. It is worth noticing, the technique could be instead easily implemented to mitigate the falsification effect if each vehicle i in the platoon is also equipped with additional on-board sensors (such as radar, lidar) that measure the state variable of the predecessor $i-1$. In this special case, the voting algorithm could fuse sensor data together with wireless-transmitted information. However the use of proximity sensors, mixed to wirelessly transmitted information, is beyond this work.

To further test the robustness of our approach and to reveal its limits, we consider a worst case in which all vehicles are subjected to the previously described spoofing attack on acceleration signal. Results refer to the exemplar case of the BR topology in absence of the voting-based detection algorithm, and show that the platoon crashes after 20 $[s]$ from the beginning of the attack (see Figure 6.4). Conversely, the malicious effects can be effectively mitigated when the voting technique is exploited. Indeed, all vehicles are now able to avoid collisions, as shown in Figure 6.5a, and to track the leader velocity profile (see results in Figure 6.5b and Figure 6.5c). Note that this example has been reported with the aim to show the good performance of the proposed approach since in the real implementation of vehicles platooning, the management system owns a low level strategy for managing collisions which avoids their occurrence [10, 168].

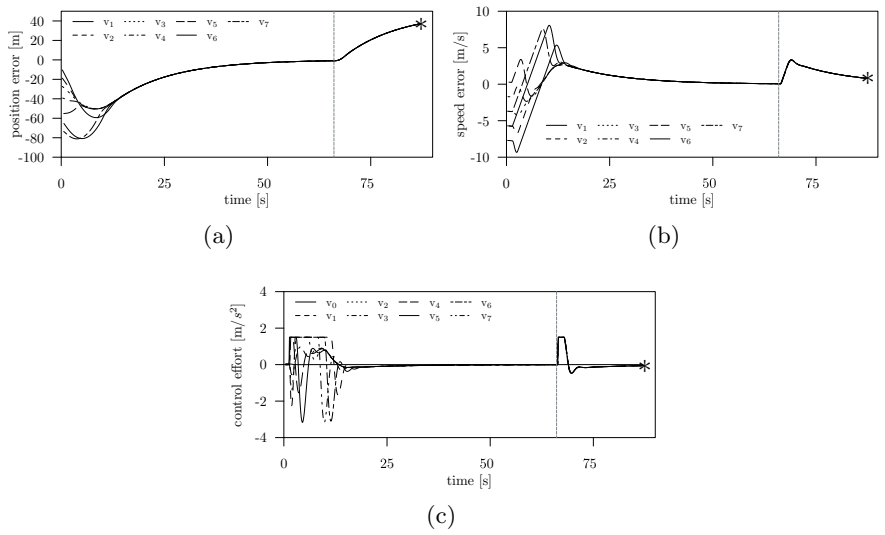


Figure 6.4: Effects of spoofing attack in nominal conditions (the malicious attack begins at time $t = 70$ $[s]$, as highlighted by the vertical gray dash line). Maintaining tight formation maneuver under BR topology: (a): time history of the position error computed as $r_i(t) - r_0(t) - d_{i0}$ $(\forall i = 1, \cdots, 7)$; (b): time history of the speed error computed as $v_i(t) - v_0$ $(\forall i = 1, \cdots, 7)$; (c): time history of the control effort $a_i(t)$ $(\forall i = 0, \cdots, 7)$. The symbol $'*'$ indicates the time instant when vehicles collide.

Message Falsification Here we consider that, at $t = 70$ $[s]$, the forth vehicle of the platoon falsifies the position field of the messages to be sent as detailed in Section 6.5.2.2. All the other vehicles accept the falsified information and then exploit them for the actuation of the longitudinal control. Consider again at first that the voting algorithm is not enabled, i.e. $\mathcal{M} = \emptyset$ in (6.4) $\forall i$. Results in Figure 6.6 show, in the case of L-P-F topology, that position errors of vehicles $5 - 6 - 7$ do not converge to zero and hence the correct tight formation is not guaranteed. Note that, as expected, a position falsification mainly influences the inter-vehicular distance (effects on speed and acceleration errors are negligible as shown in Figure 6.6b and in Figure 6.6c). Similar results have been observed for the B-F-L and BR topologies under investigations and hence they

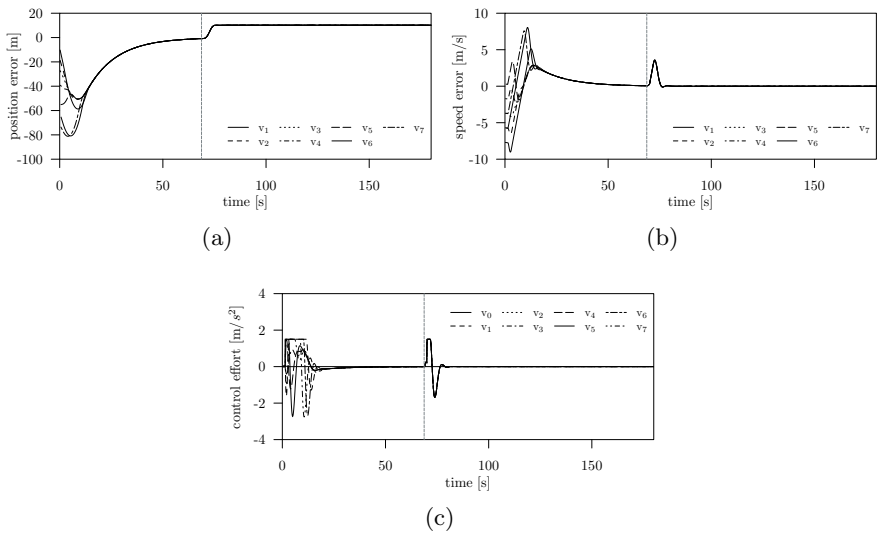


Figure 6.5: Spoofing attack (the malicious attack begins at time $t = 70$ $[s]$, as highlighted by the vertical gray dash line). Maintaining tight formation maneuver under BR topology: (a): time history of the position error computed as $r_i(t) - r_0(t) - d_{i0}$ $(\forall i = 1, \cdots, 7)$; (b): time history of the speed error computed as $v_i(t) - v_0$ $(\forall i = 1, \cdots, 7)$; (c): time history of the control effort $a_i(t)$ $(\forall i = 0, \cdots, 7)$.

are omitted here for the sake of brevity. The impact of this attack is instead more strong for the P-F topology since in this configuration each vehicle receives only data from the preceding vehicle and, hence, it can not merge alternative information to create its belief. However results are similar to Figure 6.6.

Figure 6.7 shows the results obtained in the same scenario, but with the remarkable difference of exploiting voting as a countermeasure to detect malicious behavior. Note that, differently from the previous results, now vehicle 5 is able to discard the falsified message, sent by the 4-th vehicle, and exploits only the information sent by the leading vehicle for cooperative driving. As a consequence, vehicles $6 - 7$ do not receive misleading information and the tight formation goal is still preserved. Finally we remark that the algorithm reacts to the message falsification

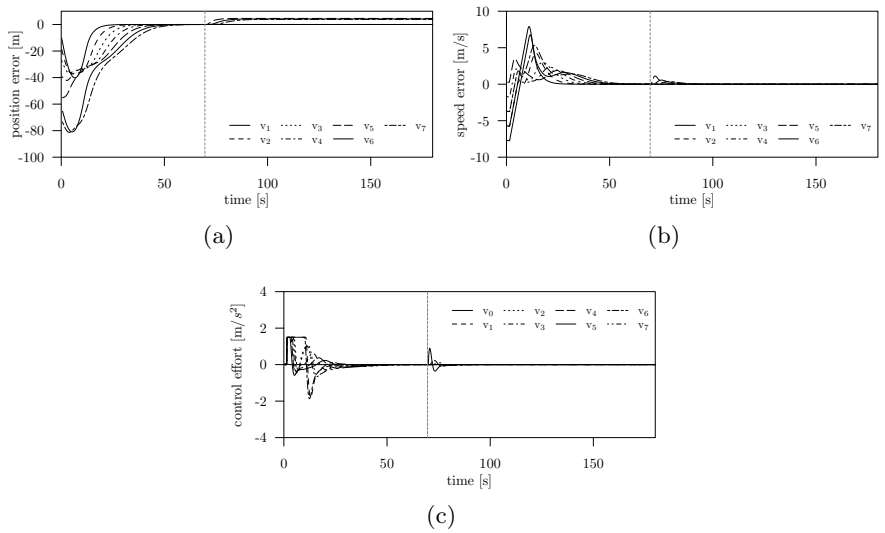
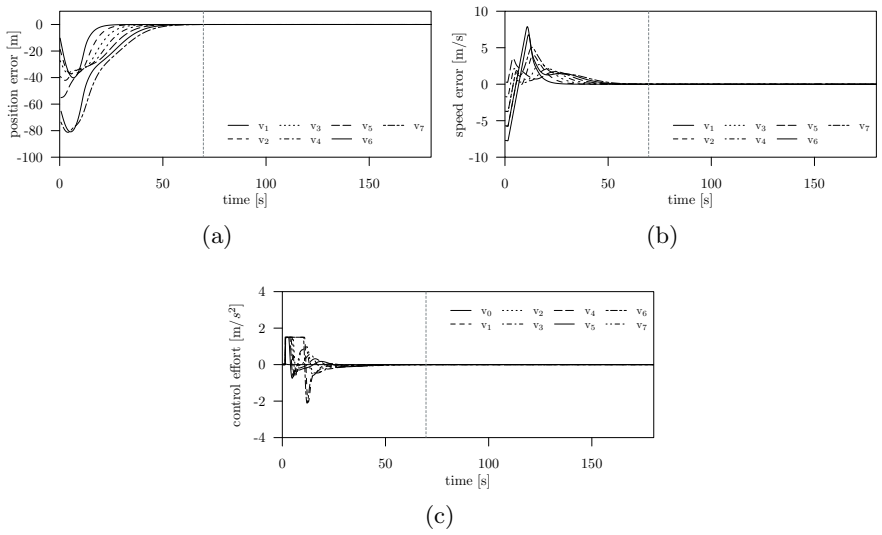


Figure 6.6: Effects of message falsification attack in nominal conditions (the malicious attack begins at $t = 70$ $[s]$ as highlighted by the vertical gray dash line). Maintaining tight formation maneuver under L-P-F topology: (a): time history of the position error computed as $r_i(t) - r_0(t) - d_{i0}$ $(\forall i = 1, \cdots, 7)$; (b): time history of the speed error computed as $v_i(t) - v_0$ $(\forall i = 1, \cdots, 7)$; (c): time history of the control effort $a_i(t)$ $(\forall i = 0, \cdots, 7)$.

attack between 0.019 $[s]$ and 0.021 $[s]$.
Similar good performance has been also observed for the B-L-F and BR topologies and results are hence omitted. As well as for spoofing attacks in P-F topology, the effects of message falsification could be limited by exploiting local sensor measurement in the voting technique. However this possibility is beyond this work.

Denial of Service Consider the DoS attack described in Section 6.5.2.3. The attack on the third vehicle starts at $t = 2$ $[s]$ for the L-P-F platoon topology.
As already mentioned, for this case of network attacks, the aim of the control protocol is not to discard false information by voting, but to compensate the lack of information due to communication impairments



(a) (b) (c)

Figure 6.7: Message falsification attack (the malicious attack begins at $t = 70$ $[s]$ as highlighted by the vertical gray dash line). Maintaining tight formation maneuver under L-P-F topology: (a): time history of the position error computed as $r_i(t) - r_0(t) - d_{i0}$ $(\forall i = 1, \cdots, 7)$; (b): time history of the speed error computed as $v_i(t) - v_0$ $(\forall i = 1, \cdots, 7)$; (c): time history of the control effort $a_i(t)$ $(\forall i = 0, \cdots, 7)$.

(packet losses). To this aim our strategy in (6.4) exploits the current delay information, $\tau_{ij}(t)$, that are detected from timestamps embedded into the GPS signal. When a message is lost, the algorithm uses the last available information, thus $\tau_{ij}(t)$ actually jumps to a large value, then returns to a smaller value when the next valid message is received.
Results in Figure 6.8 confirm the robustness of the approach and show that the maintenance of tight formation is guaranteed after a transient of 60 seconds, despite a loss rate of 30% for the third vehicle. Only the transient performance is slightly deteriorated during platoon formation maneuver. Similar good results have been obtained for the other communication topologies under investigation (and thus they are not shown for the sake of brevity).

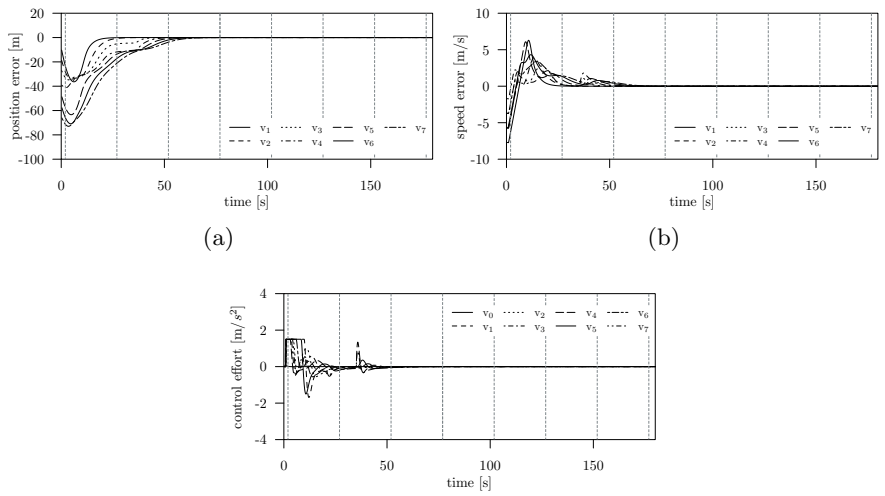


Figure 6.8: DoS attack (the malicious attack begins at $t = 2$ $[s]$ with a time duration of 20 $[s]$ and it is then repeated in a periodic fashion every 25 $[s]$ as highlighted by the vertical gray dash lines). Maintaining tight formation maneuver under L-P-F topology: (a): time history of the position error computed as $r_i(t) - r_0(t) - d_{i0}$ $(\forall i = 1, \cdots, 7)$; (b): time history of the speed error computed as $v_i(t) - v_0$ $(\forall i = 1, \cdots, 7)$; (c): time history of the control effort $a_i(t)$ $(\forall i = 0, \cdots, 7)$.

Burst Transmission In this network attack, described in Section 6.5.2.4, an adversary, external/internal to the platoon, manipulates the data traveling on wireless networks (at time instant $t = 3$ $[s]$) with the intent of dispersing some of the information necessary for collaborative driving. Also in this case, results for the L-P-F topology in Figure 6.9 confirm the algorithm effectiveness of the proposed control strategy when each vehicle within the platoon receives a percentage of the messages exchanged that randomly varies between 40% and 60%.
Although the transient performance is deteriorated with respect to the ideal case without any attack in Figure 6.1, the approach is still able to reach the reference behavior given by the leading vehicle (see Figure 6.9b) and to maintain the desired inter-vehicular spacing policy (see

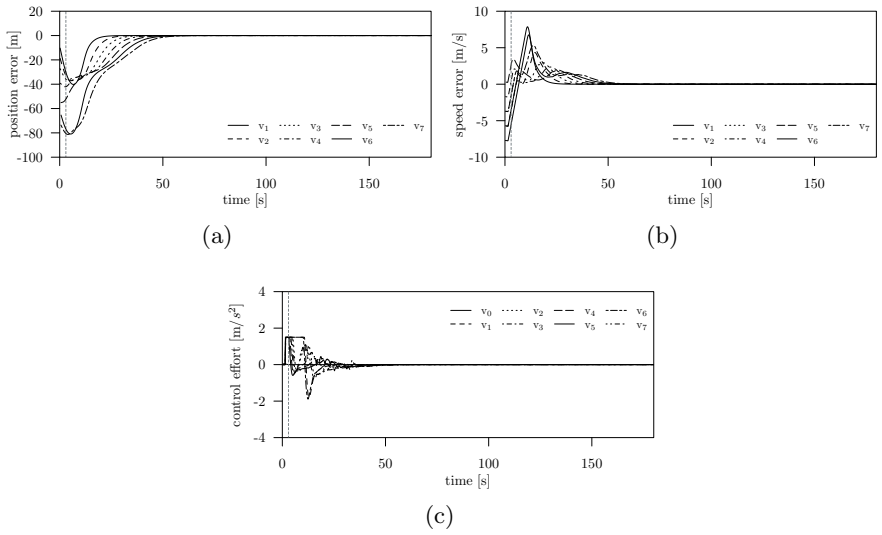


Figure 6.9: Burst attack (the malicious attack begins at time $t = 3$ $[s]$ as highlighted by the vertical gray dash line). Maintaining tight formation maneuver under L-P-F topology: (a): time history of the position error computed as $r_i(t) - r_0(t) - d_{i0}$ $(\forall i = 1, \cdots, 7)$; (b): time history of the speed error computed as $v_i(t) - v_0$ $(\forall i = 1, \cdots, 7)$; (c): time history of the control effort $a_i(t)$ $(\forall i = 0, \cdots, 7)$.

Figure 6.9a).
These robustness features with respect to burst attacks have been also observed for the other communication topologies under investigation (not shown for the sake of brevity). It is worth to note here that the Burst Transmission scenario also fits for situations that are not related to malicious attacks, as when an involuntary communication impairment happens (e.g. passing under a tunnel).
Finally, we analyze the particular case of the radio jamming attack on the overall communication network. In our scenario the adversary, at $t = 1$ $[s]$, deliberately disrupts the communication among vehicles. We suppose that the time duration of the radio jamming is limited to a specific time interval, i.e. 5 $[s]$, after which the communication is re-established. The radio jamming attack is then repeated again and again

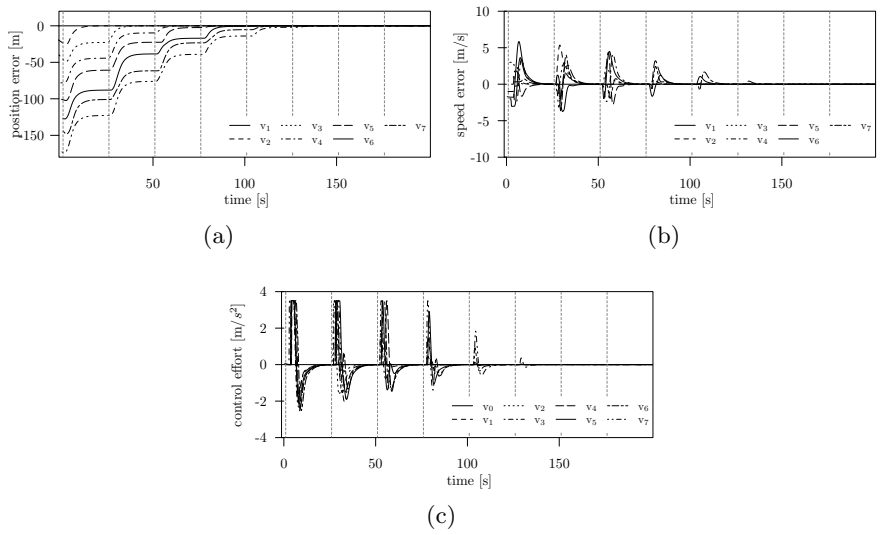


Figure 6.10: Radio Jamming attack (the malicious attack begins at time $t = 1$ $[s]$ with a time duration of 5 $[s]$ and it is then repeated in periodic fashion every 20 $[s]$ as highlighted by the vertical gray dash lines). Maintaining tight formation maneuver under L-P-F topology: (a): time history of the position error computed as $r_i(t) - r_0(t) - d_{i0}$ $(\forall i = 1, \cdots, 7)$; (b): time history of the speed error computed as $v_i(t) - v_0$ $(\forall i = 1, \cdots, 7)$; (c): time history of the control effort $a_i(t)$ $(\forall i = 0, \cdots, 7)$.

in a periodic fashion every 20 $[s]$. Furthermore, we suppose that, during the communication re-establishment, the network is subjected to a Burst attack with a loss rate equal to 80 %. Results in Figure 6.10 disclose the robustness of the proposed control strategy in bearing the total disruption of communication for 5 $[s]$ and in counteracting the losses of information due to the burst attack. In fact, although the performance are strongly deteriorated with respect to the nominal condition, the tight formation of the platoon is guaranteed after 150 $[s]$. Note that the time duration of the communication disruption, equal to 5 $[s]$, represents a threshold after which a collision could occur. However, since the maximum value of human reaction time is ≈ 0.4 $[s]$ [206], the found threshold allows human driver to get the command of the vehicle before an eventual

collision happens. Moreover, note that connected vehicles are usually equipped with additional collision avoidance systems that also include human-driver warnings (e.g. see [12] and reference therein) and, hence, at any time the driver can take the control of the vehicle in which he/she is.

6.5.3.3 Leader Velocity Tracking Performance

Here, we further test the ability of the proposed strategy to counteract a malicious attack in the case when the leading vehicle performs a longitudinal maneuver. It accelerates according to the following trapezoidal speed profile: from 0 $[kmh^{-1}]$ to 100 $[kmh^{-1}]$ with a constant acceleration of 1.5 $[ms^{-2}]$. Then it decelerates to 18 $[kmh^{-1}]$, at $t = 120$ $[s]$, with a constant deceleration of -1.5 $[ms^{-2}]$. The analysis is conducted for all the malicious scenarios presented in Section 6.5.2 and for all topologies under investigation. Here we show results achieved only in the case of L-P-F topology, since similar performance has been obtained for all the others.
Results in Figure 6.11 show that all vehicles within the platoon are able to follow the leading dynamics and to correctly track the required velocity profile in the presence of each of the malicious attacks under investigation.

6.5.3.4 A Discussion with Respect to Literature

Here we discuss the performance of our collaborative approach with respect the one proposed in [10] and then analyzed with respect to security attacks [11]. In [10] CACC (Cooperative Adaptive Cruise Control) vehicles use a one-vehicle look-ahead communication scheme where each vehicle is listening to beacon messages sent wirelessly from its immediate preceding vehicle (the communication topology is fixed). The vehicles then utilize the speed, position, acceleration, and all the other information embedded in these beacon messages, as well as on-board radar measurements for platooning. In particular, the preceding acceleration vehicle is obtained using wireless communication, while speed and inter-vehicular distance by using radar measurement (that are hence not affected by unavoidable communication delays).
The robustness with respect to security attacks is investigated by using

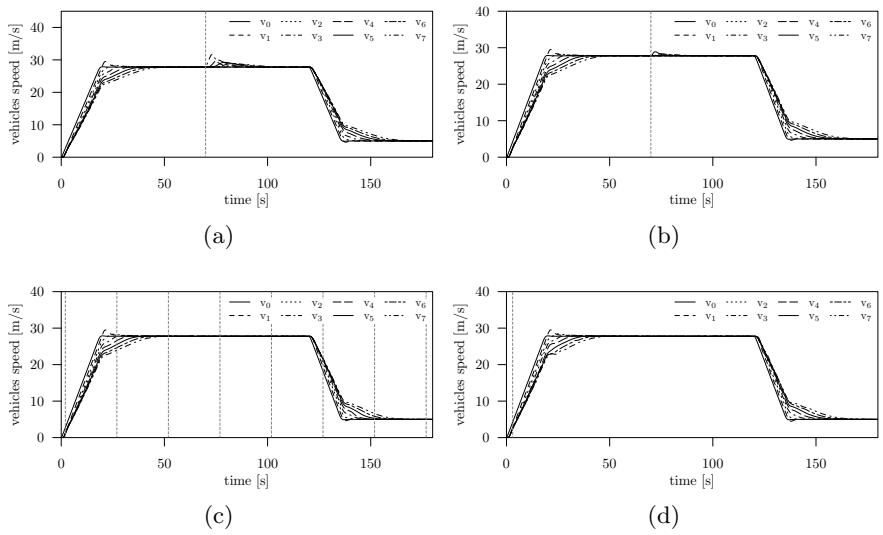


Figure 6.11: Leader tracking maneuver under L-P-F topology. Time history of vehicles speed, $v_i(t)$ ($\forall i = 0, \ldots, 7$): (a): spoofing attack; (b): message falsification attack; (c): DoS attack; (d): burst attack. The vertical gray dash lines indicate the time instant when a malicious attacks begins.

the VENTOS platform. The main results achieved in [11] can be summarized as: i) a manipulation of the acceleration field of beacon messages leads to string instability of the stream since no security features are implemented in vehicles; ii) when a radio jamming occurs, the only solution for its mitigation is the downgrading of the control strategy to non cooperative ACC approach.

Our approach enhances the cooperative driving problem in the presence of malicious attacks in several different ways. First, we consider only wireless information about position and speed of the vehicles for cooperative driving achievement and we model explicitly, in analytical way, the V2V communication time-delay. Indeed, in practice, vehicles share information through dedicated wireless communication networks. Hence, time-delays in data acquisition and transmission are unavoidable [164]. Furthermore, communication time-delays can not be assumed as uniform (homogeneous) and constant, but they have to be considered

as time-varying functions depending from the specific communication link under investigation [30] (multiple, or heterogeneous, time-varying delays).
Second, our strategy overcomes the limitation of V2V communication structure in [11], restricted only to P-F.
Third, differently from [11], we have considered in our analysis four attacks, explaining their effects, proposing and then implementing solutions for their mitigation. Indeed, we proposed a novel, secure and robust, distributed strategy that embeds a collaborative decision-making technique, able to promptly counteract the cyber attacks. Using the PLEXE platform we performed a meticulous analysis on the effectiveness of the proposed strategy for different leader driving maneuvers and for different communication topologies. Comparing the results in [11] with those presented in Section 6.5.3.2 and Section 6.5.3.3, we can observe the robustness of our approach to the malicious attacks: the stability of the stream is still preserved, hence guaranteeing the cooperative driving in the presence of cyber threats.

6.6 Concluding Remarks

In this chapter, the problem of cooperative driving for vehicles platoon in the presence of security vulnerabilities in vehicular networks is addressed. To avoid dangerous implication for safety it is fundamental, first to identify the effects deriving from a malicious attack and then to consider them in the control strategy design. Based on the study of messages alteration and communication impairment attacks, we proposed and validated a novel, robust, consensus-based control strategy mixed to a voting technique. We have analytically proven the stability of the decentralized control in the presence of time-varying communication delays and cyber threats by exploiting the Lyapunov-Krasovskii approach. The hi-fidelity analysis, conducted with the PLEXE simulator, confirmed the theoretical derivation, the robustness to vulnerabilities and the good responsiveness in reacting to the malicious attack. Finally, the strategy has been qualitatively compared with a classic CACC approach, well known in literature. The comparison has highlighted the superiority of our approach and the enhancement with respect to the state of art.

CHAPTER 7

Cooperative Driving at Traffic Junction

In this chapter, we focus on cooperative driving of autonomous vehicles approaching a traffic junction. The cooperative crossing application is addressed by recasting the intersection geometry as a virtual platoon and solved by leveraging a distributed finite-time controller that exploits outdated information, shared via the new brand $5G$ communication network, to proper compute its action. The stability of the closed-loop is an on-going work and hence not reported here. Numerical simulations disclose the effectiveness of the control approach in guaranteeing the cooperative crossing of autonomous vehicles at traffic junction without collisions.

7.1 Cooperative crossing of autonomous vehicles as virtual platoon problem

Urban traffic intersection accounts for a significant part of traffic accidents and their appropriate management is a challenge for transportation system research, due to its potential to increase road safety while decreasing traffic congestion [145]. To face this issue, intelligent traffic lights, that dynamically adapt the traffic signals to the actual traffic condition, have been proposed in the technical transportation literature (see [95] and

references therein). Nevertheless, the effectiveness of these approaches strongly relies on correct human reactions and hence, nowadays, the percentage of accidents at intersections are still very high [178].
On the other hand, self-driving cars, connected through wireless communication technologies, have been recently proposed as a promising solution to enhance the road safety and to improve the traffic efficiency [43]. In this context, leveraging Vehicle-to-Everything (V2X) paradigm (based on the protocol IEEE 802.11p), or the newly mobile communication networks 5G, the connection among vehicles and/or roadside infrastructures enables a global environmental perception, easily including the presence of other road users both within and beyond the line of sight [114].
Real-time information exchange empowers the cooperation among autonomous vehicles that hence can explicitly coordinate their mutual actions in order to avoid collisions or optimize the overall on-the-road performance [34]. Among the cooperative autonomous driving techniques, the handling of vehicular platoons has been recognized as a suitable solution for traffic congestion avoidance in the very next future [96, 66, 155, 170]. It follows that these cooperative abilities can be also exploited for dealing with the safe management of groups of autonomous vehicles negotiating a traffic junction without the intervention of any traffic light.
In the wide technical literature on connected autonomous vehicles, the different techniques for the safe intersection crossing have been mainly categorized as *centralized* and *decentralized* (see [165] and references therein). In centralized approaches, an Intersection Coordination Unit (ICU) acts as a supervisor that globally coordinates all vehicles tasks in order to minimize the risk of collisions and/or the travel time [221, 195, 99, 157]. However, when considering an intersection involving a large number of autonomous vehicles, this centralized control architecture may result unsuitable because of both its limitation to gather and process a large amount of information and the difficulty arising from solving in real-time the consequent large-scale optimization problem [214].
Differently, decentralized approaches, where each vehicle determines its dynamic behavior on the basis of only information received by neighbors, implement at single vehicle level decision making algorithms allowing to negotiate the access to the traffic intersection. Once the crossing time or

order is scheduled, a control strategy locally provides the required acceleration/deceleration profile that each vehicle has to track. Optimal control approaches, tailored for the specific geometry of a given road intersection, are usually exploited for accounting the hard safety constraints necessary to avoid collisions, as for example in [208, 93, 43, 126, 209]. Note that these optimization approaches are usually proven only through numerical simulations since their real-time deployment may require some heuristic approximations to deal with the combinatorial complexity of the search algorithm.

In order to provide flexibility with respect to the intersection geometry, very recent approaches for control design leverage coordinate transformation to recast the crossing problem as the control of a virtual longitudinal platoon that opportunely arranges the vehicles that may be in different lanes of the junction and may have different directional intentions. Specifically, this recast has been proposed in the seminal work [188] and recently exploited in [132], where a just simulation study shows the performance of a classical longitudinal (virtual platooning) controller based on a linear CACC strategy which is essentially an inter-vehicle distance control algorithm that ensures the string stability, i.e. ensures that once at steady-state, the inter-vehicular distances are kept constant. However, for safety reasons, a fundamental problem is to guarantee, from the very beginning of control design, that the desired virtual formation is effectively reached before vehicles enter the Conflicting Area (CA), i.e. the intersection core area where collisions could occur (see Fig. 7.1 and the definitions in the following Sec. 7.2).

To face this issue, this chapter propose a completely distributed nonlinear finite-time control strategy for cooperative vehicles negotiating an intersection. Collisions are, hence, prevented due to the achievement of the desired virtual formation in a finite time T before the first vehicle accesses the CA. Moreover, the control protocol guarantees desired inter-vehicle distances among virtual platoon members such that real vehicles access the CA in a mutually exclusive fashion, while the simultaneous achievement of a common platoon velocity ensures that the desired formation will be preserved once reached.

The effectiveness of the proposed approach is validated in numerical way.

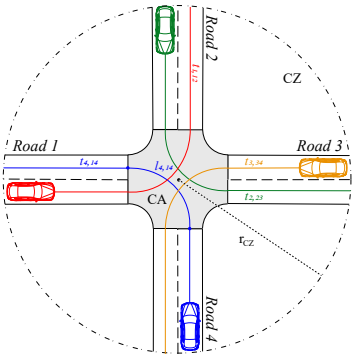


Figure 7.1: A possible traffic junction scenario ($\mu = 4$). Vehicles cooperate for autonomously and exclusively crossing the Conflicting Area (CA). Once inside the Cooperative Zone (CZ), the vehicle i chooses one of the possible trajectories $t_{i,pq}$ starting from the road p where they are initially located.

7.2 System Modeling and Problem Formulation

Consider a scenario where N vehicles are autonomously driving along μ different two-lane roads leading into a traffic junction, regulated neither by traffic lights or ordinary traffic rules, as depicted in Fig. 7.1. The central polygonal zone (highlighted in gray), is the Conflicting Area (CA) which represents the intersection core area where collisions could occur, while the larger circular zone with radius r_{cz} is referred as Cooperation Zone (CZ).

We assume that each self-driving vehicle i ($\forall i = 1, \cdots, N$) is able to measure its own position and speed exploiting onboard sensors and hence to act accordingly on its acceleration/braking control systems for following, also thanks to onboard steering, its own trajectory $t_{i,qg}$ linking the road q, where the vehicle is initially located, with the road g, where the vehicle is heading to.

Moreover, we assume that each vehicle i approaching the traffic junction is modelled by the second-order longitudinal dynamics in (3.3), i.e.

$$\dot{p}_i(t) = v_i(t) \tag{7.1}$$

$$\dot{v}_i(t) = \frac{1}{m_i} u_i(t), \tag{7.2}$$

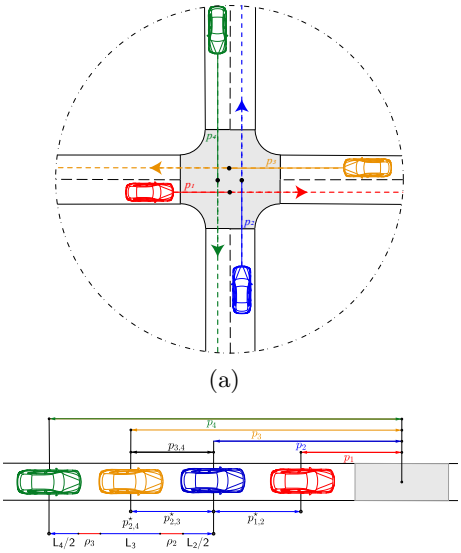


Figure 7.2: Autonomous vehicles approaching the traffic junction as a virtual platoon problem w.r.t. the position from the centre of the chosen trajectory $p_i(t)$. a) Computation of the $p_i(t)$. b) Virtual platoon recast and choice of the desired distance according to Algorithm 2.

being $p_i(t)$ the position of each vehicle i, expressed as its distance from the center of its trajectory $t_{i,qg}$ (as shown in Fig. 7.2), $v_i(t)$ its velocity and m_i its mass.
In addition, vehicles within CZ are assumed to be connected via the brand new $5G$ mobile communication network in order to share information about their own trajectory and their local state. The communication topology in the CZ can be hence described by a directed connected graph $\mathcal{G}_N$ even though not completely connected.
The final aim is to regulate the motion of each vehicle so that the autonomous connected vehicles, cooperating through exchanging information in the CZ, cross the CA with a mutually exclusive mode in order to avoid side and rear-end collisions [196], i.e. at most one vehicle must drive without stopping within the CA at any time instant. Note that, the

traffic flow may arrive quite continuously at a road intersection. However, for a specific time interval, we only need to consider a restricted group of N vehicles that are moving to the junction [113]. Under this consideration, as shown in Fig. 7.1, vehicles inside the CZ will be considered as the group that currently takes part in cooperative crossing, whereas vehicles outside the CZ will be postponed to the next negotiating.

7.2.1 Problem Formulation as a Virtual Platoon

In order to solve the coordination problem described above, in what follows we formulate it as a virtual longitudinal platoon control problem. The core idea is to re-organize and control all vehicles driving within the CZ as a virtual platoon, ordered on the basis of the distance $p_i(t)$ of each vehicle from the center of its trajectory, $t_{i,qg}$ $\forall i = 1, \cdots, N$ (as shown in Fig. 7.2). Details on the coordinate transformations and mathematical manipulations that allow to map the vehicle coordinate vector $r_i(t)$, provided by the GPS receiver, into the position $p_i(t)$ along the trajectory and the relative positions $p_{ij}(t)$ between vehicles i and j ($i, j = 1, \cdots, N$ with $i \neq j$) are reported in [132].
The vehicles ordering into the platoon w.r.t. $p_i(t)$ clearly corresponds to a crossing order, so that the closest vehicle crosses first. Both side and rear-end collision avoidance is achieved by ensuring the desired spacing policy within the virtual formation, i.e. vehicles have to reach and maintain pre-fixed inter-vehicular gaps as they drive with a common velocity. Specifically, the desired inter-vehicle distances imposed among virtual platoon members, say $p^{\star}_{ij}$ ($\forall(i, j)$), have to be selected so to ensure that real vehicles access exclusively the CA, while the achievement of a common velocity guarantees that the desired formation will be preserved once reached. It is important to highlight that collisions are prevented by the achievement of the desired formation in a finite time T before the first vehicle enters into the CA.
The Virtual Platoon control objective that recasts the problem of self-driving cars negotiating their way through the intersection can be now summarized as follows. Given the virtual platoon, obtained by organizing the N vehicles within the CZ in ascending order of distances from the center of their trajectories $p_i(t)$ ($\forall i = 1, \cdots, N$), find a distributed

cooperative control protocol $u_i(t)$ such that $\forall(i,j)$ the achievement of the following desired formation is guaranteed in a finite-time T:

$$|p_i - p_j| \to p_{ij}^{\star}, \tag{7.3}$$

$$|v_i - v_j| \to 0, \tag{7.4}$$

being $p_{ij}^{\star}$ the desired inter-vehicular gaps (calculated according to Algorithm 2).

7.2.2 Procedure details

The implementation of the proposed methodology consists of two steps: an initialization phase, performed one-time at the entrance of the CZ, and a cyclic routine.

During the initialization phase, vehicles have to perform the following tasks: (a) agreeing on a common order into the virtual platoon on the basis of the exchanged messages; (b) calculating the desired relative distances $p_{ij}^{\star}$ that ensure the exclusive access into CA.

During the cyclic routine, instead, the following tasks have to be executed by each vehicle i: (c) locally measuring its position and velocity and then computing the position along its trajectory $p_i(t)$; (d) receiving/sending local state information from/toward vehicles connected via the $5G$ network and calculating the relative distances w.r.t each vehicle j in the neighboring set (see Fig. 7.2b); (e) actuating the acceleration control input $u_i(t)$ according to a virtual platoon protocol. Note that, the desired inter-vehicle distances (task (b)) have to be selected so that the platoon formation guarantees when a vehicle leaves the CA, the next one is just ready to enter (see figure Fig. 7.2). For this purpose, Algorithm 2 provides the values $p_{ij}^{\star}$ according to vehicle length L_i $(i = 1, \cdots, N)$ and vehicle trajectory $t_{i,qg}$ at the intersection geometry.

Algorithm 2: Computing the desired inter-vehicles gap for the vehicle i

Let $\xi_i = l_{i,qg}$ be the length of the trajectory followed by the the i-th vehicle when it crosses the intersection from road q to road g.
Define $d_{i,i-1} = \frac{L_i}{2} + \frac{L_{i-1}}{2}$, being L_i the length of the i-th vehicle
if $i > j$ **then**
  $p^{\star}_{ij} = \sum_{i=i+1}^{j} [d_{i,i-1} + \xi_{i-1}]$
if *;*
then
  $i < j$
$p^{\star}_{ij} = \sum_{i=j+1}^{i} [d_{i,i-1} + \xi_{i-1}]$

7.3 Distributed Finite Time Control Protocol for Self-driving Vehicles at Intersection

In order to solve the problem of the cooperative driving at traffic junction, we propose the following distributed nonlinear control law:

$$\begin{aligned} u_i(t) = &- \sum_{j=1}^{N} a_{ij} sig(p_i(t-\tau_{ij}(t)) - p_j(t-\tau_{ij}(t)) - p^{\star}_{ij})^{\frac{2\alpha}{1+\alpha}} \\ &- \sum_{j=1}^{N} a_{ij} sig(v_i(t-\tau_{ij}(t)) - v_j(t-\tau_{ij}(t)))^{\alpha}, \end{aligned} \tag{7.5}$$

where $\alpha \in (0;1)$ and $sig(x)$ is defined as [129, 22]:

$$sig(x)^{\alpha} = sign(x)|x|^{\alpha}, \tag{7.6}$$

being $x \in \mathbb{R}$ and $sign(\cdot)$ is the signum function. Moreover, a_{ij} models the topology of the underlying connected communication graph $\mathcal{G}_N$, i.e. the presence/absence of a communication link between the i-th and j-th vehicle; $\tau_{ij}(t)$ models the unavoidable communication time delay affecting information shared among vehicle i and vehicle j via the 5G communication link (i,j) ($\forall i = 1, \cdots, N \; \forall j = 1, \cdots, N, i \neq j$). Hence, communication time-delays are assumed to heterogeneous, i.e. different for each communicating link (i,j), and time-varying functions whose actual value, at a given time instant, depends on the current availability of the communication link [116].

Control gain α	0.1
Vehicle length L_i $[m]$	4 $(\forall i = 1, \ldots, 4)$
Length of the trajectory ξ_i $[m]$	16 $(\forall i = 1, \ldots, 4)$
Position initial condition $[m]$	
$[p_1(0), p_2(0), p_3(0), p_4(0)]^\top$	$[-212, -222, -232, -242]^\top$
Velocities initial condition $[m/s]$	
$[v_1(0), v_2(0), v_3(0), v_4(0)]^\top$	$[11, 9, 11, 9]^\top$

Table 7.1: SIMULATION PARAMETERS

7.4 Numerical Validation

Consider, as an exemplary case of study, $N = 4$ autonomous vehicles driving along 6 different two-lane roads approaching a traffic junction, as depicted in Fig. 7.1. When vehicles enter into the CZ (characterized by a radius $r_{CZ} = 250$ $[m]$) they exchange information with all the other vehicles within the area (all-to-all communication topology). On the basis of these information, the finite-time distributed control protocol (7.5), with $\alpha = 0.1$, properly acts in order to guarantee the safe crossing with the desired inter-vehicle spacing $p_{ij}^\star$ $(\forall i, j = 1, \cdots, N$ with $i \neq j)$, computed according to Algorithm 2.

The numerical analysis has been performed by exploiting the MATLAB© platform where, for the simulation scenario, communication delays have been emulated as a random time-varying functions whose maximum value is $\tau_{ij}^\star = 0.05$ $[s]$ according to the experimental analysis conducted on the $5G$ communication delay in [18]. Simulation parameters are reported in Tab. 7.1.

The time histories of vehicles positions, velocities and accelerations are reported in Fig. 7.3a, Fig. 7.3b and Fig. 7.3c respectively, while the position errors with respect to the desired inter-vehicle distances and velocities errors are shown in Fig. 7.3d and Fig. 7.3e, respectively.

Results in Fig. 7.3a and Fig. 7.3d clearly endorse the effectiveness of the finite-time proposed control strategy in ensuring that the desired inter-vehicle spacing $p_{ij}^\star$ $\forall(i, j)$ is achieved and maintained. This implies that, for any time, no more than one vehicle is into the CA, whose boundaries are indicated with the dashed-dotted horizontal lines; indeed, only when one vehicle has exited the CA, the next one is just ready to enter the intersection, as highlighted by the vertical solid lines. Moreover, once

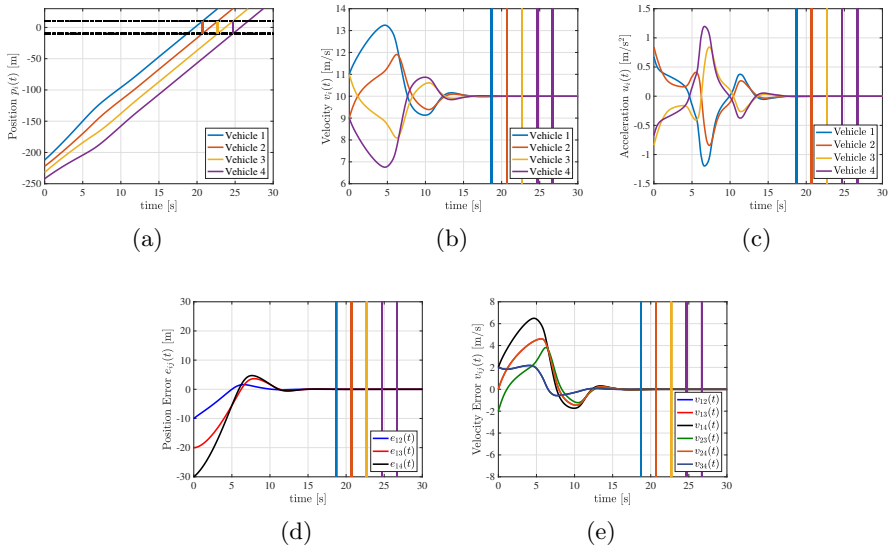


Figure 7.3: Four autonomous vehicles negotiating a six roads intersection ($i = 1, \ldots, 4$). a) Time history of vehicles positions (boundaries of the CA: dash-dots horizontal lines). b) Time history of vehicle velocity. c) Time history of vehicles accelerations. d) Time history of position errors computed as $p_i(t) - p_j(t) - p^{\star}_{ij}$, $(i, j = 1, \ldots, 4 \; i \neq j)$. e) Time history of the speed errors computed as $v_i(t) - v_j(t)$, $(i, j = 1, \ldots, 4 \; i \neq j)$. Vertical lines in figures b), c) d) and e) indicate the time instant at the witch each vehicle enters and exits the CA. Note that the different colors refer the different vehicles (some vertical line are not visible since they are overlapped)

the desired formation is obtained, the control protocol leads vehicles to the velocity consensus $v^{\star} = 10 \; [m/s]$, as depicted in Fig. 7.3b, Fig. 7.3e and Fig. 7.3c. As required, the convergence is guaranteed before the first vehicle accesses the CA, hence ensuring the absence of collisions. Indeed the cooperative crossing problem 7.3 is solved in a finite time T of about 17 [s] (chosen the control gain as $\alpha = 0.1$). Fig. 7.4 shows the inner relationship between the control parameter α and the corresponding convergence time T w.r.t to the appraised initial conditions for vehicles

position and velocities in Tab. 7.1. Note that, according to [129], the shortest convergence time occurs when α is approaching to 0 and this confirms that the control parameter α can be properly tuned so to ensure the desired convergence rate. Finally, we highlight that readers may refer to the next Chapter 8 for a more detailed discussion about the effectiveness of the proposed control strategy in real on-the-road scenarios.

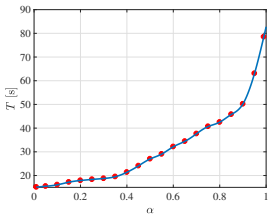


Figure 7.4: Settling time T [s] v.s. control gain $\alpha \in (0; 1)$.

7.5 Concluding remarks

In this chapter a distributed control algorithm solving the problem of coordinating autonomous vehicles at traffic intersections over $5G$ communication networks has been proposed. By re-arranging all vehicles within the cooperative zone at the intersection, the coordination problem has been first recast as a virtual platoon control problem and then solved by a distributed nonlinear control strategy, guaranteeing convergence to a safe configuration in finite-time. The closed-loop stability is an on-going work and hence not reported here. Numerical results have revealed the ability of the vehicles to negotiate the traffic intersection so to cross it without collisions.

CHAPTER 8

Experimental validation of Cooperative Driving Strategies

In this Chapter we present the experimental validation campaign that we carried out, in collaboration with Professor Paolo Falcone of Chalmers University of Technology (Gothenburg, Sweden) and the Research Department of Ericsson (Gothenburg, Sweden), to test the cooperative driving control strategy proposed in Chapter 7. Experiments were performed at AstaZero test track (near Gothenburg, Sweden) by exploiting three heterogeneous vehicles, properly equipped with specific communication and control hardware: *Volvo Car XC90*; *Volvo Car S90*; *Volvo Truck FH16*. Experimental results confirmed the effectiveness of the proposed approach in guaranteeing, in real on-the-road scenarios, the safe crossing of autonomous connected vehicles at traffic junctions.

8.1 Experimental setup

The experimental trial involves three heterogenous vehicles, i.e. Volvo Car XC90, Volvo Car S90 and Volvo Truck FH16, that exchange information via a 5G communication network, kindly provided by Ericsson. Since vehicles have been provided by Chalmers university of Technology

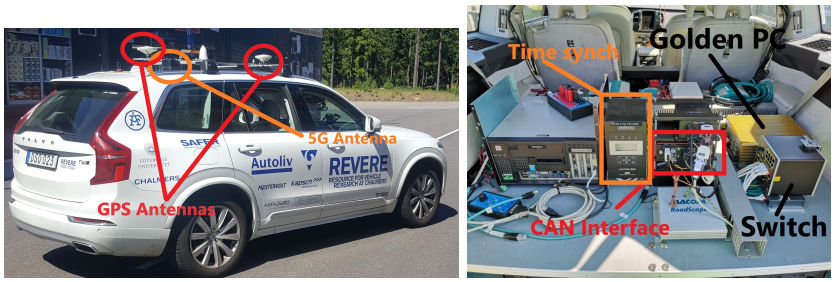
and by Ericsson, each vehicle is proper equipped with different communication/control hardware devices and software components. Vehicles are hence heterogeneous in their masses, on-board systems and driving mode.
The Volvo Car XC90 and the Volvo Truck FH16 have been kindly loaned by the Revere Laboratory of Chalmers University of Technology. They are equipped with the open-source driving system OpenDLV [20, 21, 19]. On the other hand, Volvo Car S90 has been provided by Ericsson and it is endowed with an ADB Pedal Robot [1] to drive the vehicles motion by acting on steering and throttle/brake pedals. In turn, the robot can be controlled through a proprietary interface that interfaces with Matlab Realtime. In the following we detail for each vehicle under investigation the vehicle architectures focusing both on hardware devices and software components.

8.1.1 Volvo Car XC90

Here we analyze the hardware and software components of the Volvo Car XC90 belonging to the Revere Laboratory at Chalmers and depicted in Fig. 8.1. The sensing and control subsystems, on this car, are entirely managed and supervised by OpenDLV. In particular, on-board sensors and actuators are connected, through a Local Area Netowrk (LAN), local to the car, with a main computer and exchange data through an UDP

(a) (b)

Figure 8.1: Test Car Volvo XC90: a) front perspective; b) back perspective.



(a) (b)

Figure 8.2: Test Car Volvo XC90 a) Test Car Volvo XC90 - External Instrumentation b) Test Car Volvo XC90 - Internal Instrumentation

Multicast session. The following sensors and actuators, already installed and configured on the car, are used to carry out the experiments:

- Applanix GNSS: GNSS/INSS unit providing car position data in GPS coordinates. This sensor is combined with a Radio modem to gain RTK corrections on the field achieving a precision up to centimeters in data position [194].
- Inertial Movement Unit (IMU): On-board unit that is used to assess the current vehicle acceleration.
- 5G Telit Modem: 5^{th} generation modem to establish a radio communication with the 5G Ericsson Proof of Concept network.
- 5G Antennas: 5^{th} generation antennas to receive information coming from the 5G Ericsson Proof of Concept network.
- CAN Interface: Interface to the vehicle CAN to receive information related to the current speed and send to the vehicle ECU the computed control signals.
- Time-Synch: Time Synchronize used to align the clock among multiple devices.

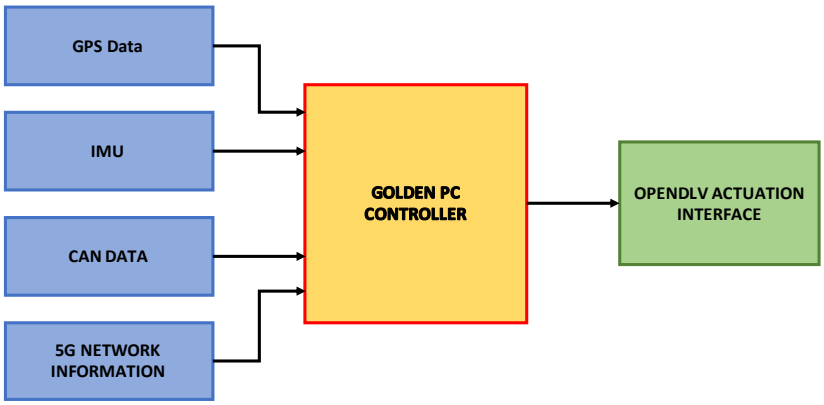


Figure 8.3: Software architecture executed on OpenDLV.

- Golden PC: Main computer running the OpenDLV software under a GNU/Linux based operating system (ArchLinux) to handle autonomous driving sensing and actuating software. This computer computes the control input on the basis of on-board and network information.

This hardware configuration is showed in Figure 8.2a and 8.2b. The software architecture, executed on OpenDLV, is instead depicted in Fig. 8.3. Here, the blue boxes represent measurements and communication interfaces, while the yellow box implements the cooperative driving control strategy. The green one, instead, is the vehicle interface to the powertrain. This architecture is hierarchical, i.e. it is composed by an upper and a lower level controller. The upper level (designed in this thesis), leveraging data received from neighbors and local information, determines the desired acceleration that has to be imposed for achieving the required formation, while the Actuation Interface on OpenDLV passes the appropriate commands to the powertrain, so that the lower level control can command the throttle and/or brake system of each vehicle for the actuation of the reference acceleration profile.

8.1.2 Volvo Truck FH16

Here we analyze the hardware and software components of the Volvo Truck FH16, belonging to the Revere Laboratory at Chalmers and depicted in Fig. 8.4. The autonomous driving on-board system on this

vehicle is quite similar to the one of the XC90. Infact, the sensing and control subsystems on the truck are entirely managed and supervised by OpenDLV. In particular on-board sensors and actuators are connected, through a Local Area Netowrk (LAN), local to the vehicle, with a main computer and exchange data through an UDP Multicast session. The following sensors and actuators, already installed and configured on the truck, are used to carry out the experiments:

- Oxford OXTS GNSS: GNSS/INSS unit providing position data GPS coordinates. This sensor is combined with a Radio modem to gain RTK corrections on the field achieving a precision up to centimeters for data position [194].
- Inertial Movement Unit (IMU): On-board unit that is used to assess the current vehicle acceleration.
- 5G Telit Modem: 5^{th} generation modem to establish a radio communication with the 5G Ericsson Proof of Concept network.
- 5G Antennas: 5^{th} generation antennas to receive information coming from the 5G Ericsson Proof of Concept network.
- CAN Interface: Interface to the Volvo Truck CAN to receive information related to the current speed and send the control signal.
- Time-Synch: Time Synchronize used to align the clock among multiple devices.
- Golden PC: Main computer running the OpenDLV software under a GNU/Linux based operating system (ArchLinux) to handle autonomous driving sensing and actuating software. This computer computes the control input on the basis of on-board and network information.

This hardware configuration is showed in Figure 8.5.

The software architecture, executed on OpenDLV, is instead depicted in Fig. 8.3. This architecture is hierarchical, i.e. it is composed by an upper and a lower level controller. The upper level (designed in this thesis), leveraging data received from neighbors and local information, determines the desired acceleration that has to be imposed for achieving

Figure 8.4: Volvo Truck FH16

Figure 8.5: Test Truck Volvo FH16 - Instrumentation

the required formation, while the Actuation Interface on OpenDLV passes the appropriate commands to the powertrain, so that the lower level control can command the throttle and/or brake system of each vehicle for the actuation of the reference acceleration profile.

8.1.3 Volvo Car S90

Here we analyze the hardware and software components of the Volvo Car S90, provided by Ericsson and depicted in Fig. 8.6
The vehicle exploits an ADB Pedal Robot (see Fig. 8.7) to actuate the designed cooperative driving control strategy which is proper computed

Figure 8.6: Volvo Car S90

Figure 8.7: Volvo Car S90: ADB Pedal Robot

via the dSpace Micro Autobox (MBAX)[54]. MBAX is a real-time platform that is interconnected with the vehicle and the on-board equipment through the Controlled Area Network (CAN) and the Local Area Network (LAN), respectively and programmed through the Matlab Realtime (Matlab RT) Toolbox. The control strategy is indeed implemented via Matlab RT Toolbox and the related code is then uploaded on the MBAX which elaborates the control output on the basis of network and local information. The computed control strategy is then sent to the pedal robot via the LAN. The following sensors and actuators are used to carry

Figure 8.8: Test Car Volvo S90 Instrumentation

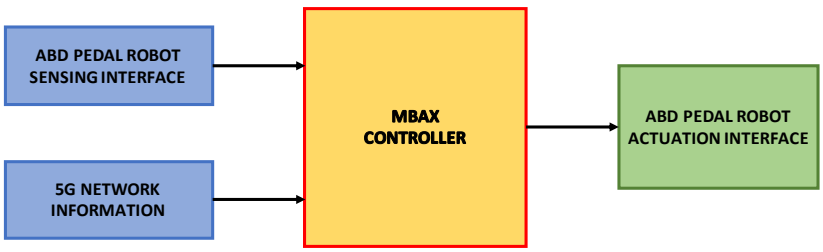


Figure 8.9: Software architecture executed on dSpace MicroAutobox.

out the experiments:

- ADB Pedal Robot: This powerful robot acts both as sensor and actuators. It has a direct connection with the vehicle GNSS unit, IMU and CAN. Therefore it can communicate to the dSpace MBAX the current state of the car. Furthermore it has the ability of actuate the vehicle acceleration and the braking system (through mechanical actuators on pedals) according to the designed and implemented cooperative driving control strategy.

- 5G Telit Modem: 5^{th} generation modem to establish a radio communication with the 5G Ericsson Proof of Concept network.

- 5G Antennas: 5^{th} generation antennas to receive information coming from the 5G Ericsson Proof of Concept network.

- Communication Box: It is a Raspberry PI opportunely programmed to receive data from the 5G network and converts them in a readable format for the dSpace MBAX.
- Router: It creates the internal ethernet LAN interconnecting all onboard components.

This hardware configuration is showed in Fig. 8.8 while the software architecture, executed on MBAX, is showm in Fig. 8.9. Here, the blue boxes represent measurements and communication interfaces, while the yellow box implements the cooperative driving control strategy. The green one, instead, is the vehicle interface to the powertrain. This architecture is hierarchical, i.e. it is composed by an upper and a lower level controller. The upper level (designed in this thesis), leveraging data received from neighbors and local information, determines the desired acceleration that has to be imposed for achieving the required formation, while the Actuation Interface provided by the ABD pedal robot passes the appropriate commands to the powertrain, so that the lower level control can command the throttle and/or brake system of each vehicle for the actuation of the reference acceleration profile.

8.2 Experimental Driving Scenario

Experimental test has been carried out at AstaZero test track (near Gothenburg, Sweden) [1] in the City Area [2]. The City area consist of 4 blocks and cover a number of different sub-areas such as:

- town centers with varying street widths and lanes, bus stops, pavements, street lighting and building backdrops;
- a road system with different kinds of test environments such as roundabouts, T-junction, return-loop and lab-area. Connections to the Rural road occur in two places.

The City area is based on a relatively flat surface and with dummy blocks that resemble buildings both to the eye and to technical aids such as radar as depicted in Fig. 8.10. One block contains space for control room

[1] http://www.astazero.com
[2] http://www.astazero.com/the-test-site/test-environments/city-area/

and warehouse for dummies. The map of the City Area is reported in Fig. 8.11

Figure 8.10: The City Area at AstaZero

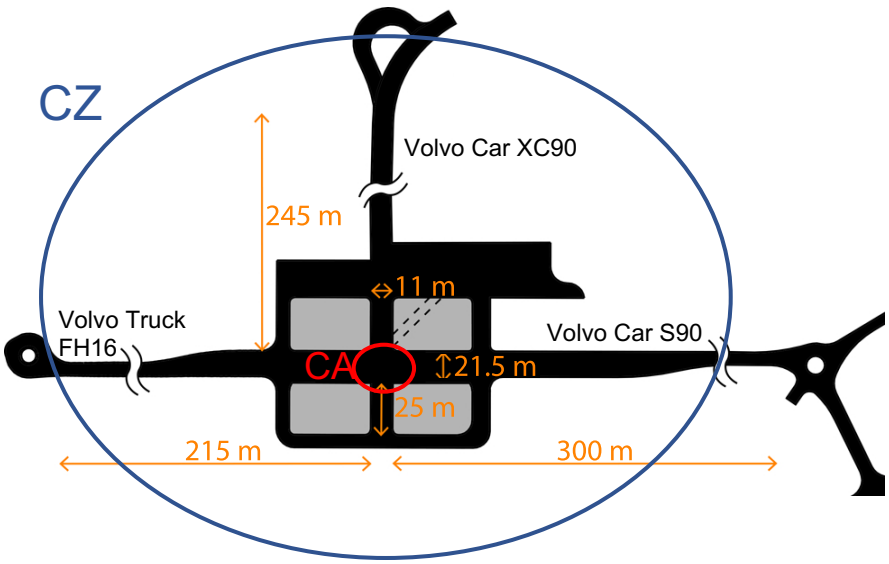


Figure 8.11: Map of the City Area at AstaZero

Herein, the Cooperative Zone (CZ) (marked with a blue circle) is the whole city area since we are considering that vehicles exchange information via 5G network. The Conflicting Area (CA) (marked with a red circle) is the T-junction part of the city. For the experimental tests, vehicles are positioned as in Fig. 8.11 and they access the CZ with a common initial velocity and relative positions that would lead to collision without any control action.
The experimental trail involves two representative cooperative driving scenarios, namely: *i*) Three autonomous vehicles scenario; *ii*) Two autonomous vehicles with one human-driven vehicle scenario. In scenario i we consider that the three vehicle are fully automated and, on the basis of the shared information, they proper act on their motion according to the control strategy in Chapter 7. In scenario ii we consider the Volvo Car XC90 and Volvo Car S90 to be fully automated while the Volvo Truck 16 to be human-driven with capability to send information about its position and speed. Parameters values, characterizing the experimental scenarios, are summarized in Tab. 8.1. Finally we highlight that the

Control parameters	
Control gain α	0.1
Vehicle length L_i $[m]$	$L_1 = 7.8 \;\; L_2 = L_3 = 4.6$
Length of the trajectory ξ_i $[m]$	10 $(i = 1, 2, 3)$
Three autonomous vehicles experimental scenario	
Position error initial condition $[m]$ $[e_{12}(0), e_{13}(0)]^\top$	$[-7.7, -10.3]^\top$
Velocities initial condition $[m/s]$ $[v_1(0), v_2(0), v_3(0)]^\top$	$[13, 13, 13]^\top$
Two autonomous vehicles with one human-driven vehicle scenario	
Position error initial condition $[m]$ $[e_{12}(0), e_{13}(0)]^\top$	$[-7.7, -10.3]^\top$
Velocities initial condition $[m/s]$ $[v_1(0), v_2(0), v_3(0)]^\top$	$[13, 13, 13]^\top$

Table 8.1: EXPERIMENTAL SCENARIOS PARAMETERS.

measured 5G communication delay is equal to $11ms$ with a standard

deviation of 0.02.

8.3 Experimental Results

The obtained experimental results, depicted in Fig. 8.12, confirm the effectiveness of the proposed control strategy in guaranteeing the safe crossing at intersection and its resiliency to communication time-delay. Indeed, each vehicle cross the CA with a mutually exclusive mode in

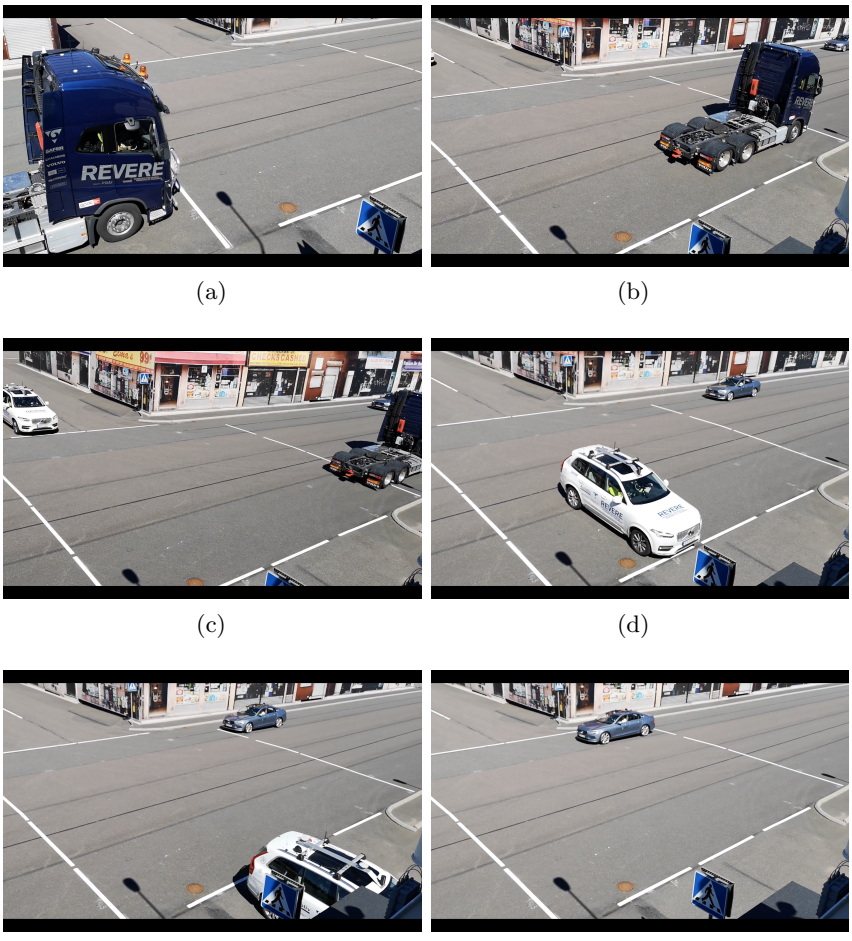


Figure 8.12: Experimental Test-05-th June 2018

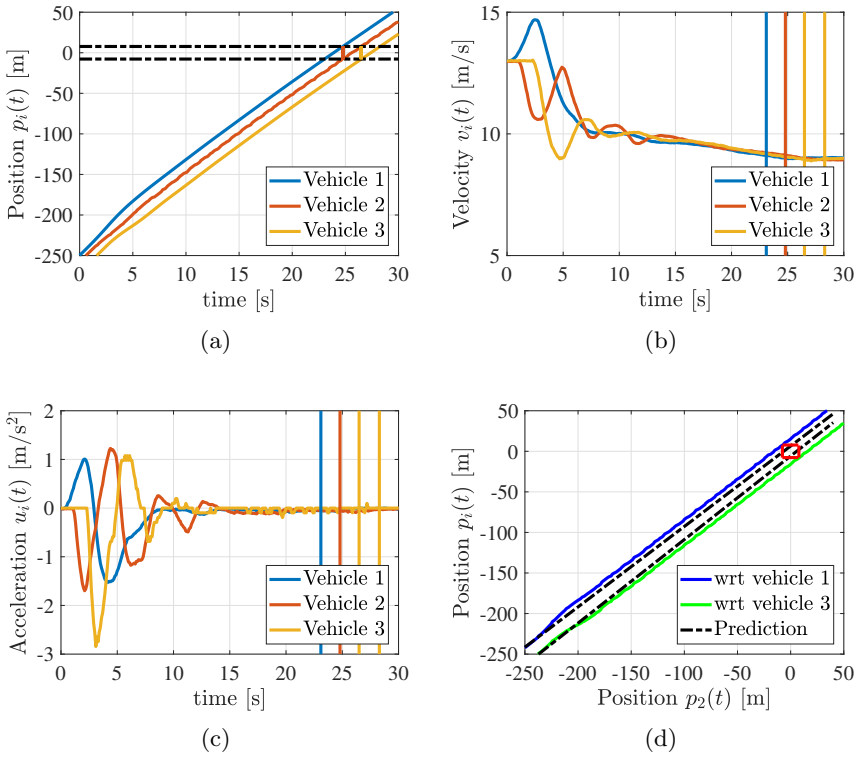
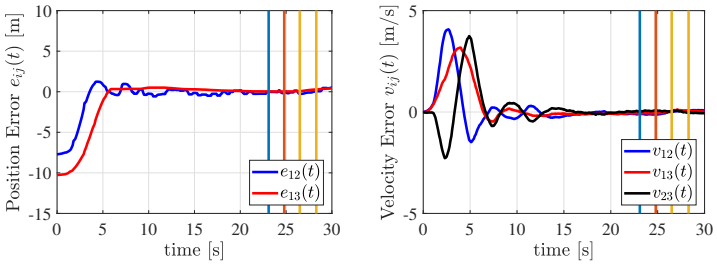


Figure 8.13: Three autonomous vehicles scenario experimental results: a) time history of vehicles positions (boundaries of the CA: dash-dots horizontal lines); b) time history of vehicles velocities; c) time history of vehicles accelerations; d): 2nd vehicle position w.r.t. 1st and 3rd vehicle positions.

order to avoid side and rear-end collisions, i.e. at most one vehicle drive without stopping within the CA at any time instant. See the full video of the experiments at `https://www.youtube.com/watch?v=rmjJkIlFMJ4`. Now we disclose in detail the experimental results obtained in the two appraised cooperative driving scenarios.



(a) (b)

Figure 8.14: Three autonomous vehicles scenario experimental results: a) time history of position errors computed as $e_{ij} = p_i(t) - p_j(t) - p^{\star}_{ij}$ $(i, j = 1, \ldots, 3\ j \neq i)$; b): time history of the speed errors computed as $v_{ij}(t) = v_i(t) - v_j(t)$ $(i, j = 1, \ldots, 3\ j \neq i)$.

8.3.1 Three autonomous vehicles scenario

Results in Fig. 8.13 and Fig. 8.14 confirm the effectiveness of the control strategy in ensuring the safe crossing of three self-driving vehicles that reach in a proper finite time the desired inter-vehicle spacing (see Fig. 8.13a and Fig. 8.14a) with a common velocity (see Fig. 8.13b, Fig. 8.14b and Fig. 8.13c) despite the presence of communication delays. Indeed, as shown in Fig. 8.14a and Fig. 8.14b, where the time histories of position and velocity errors are reported the desired control formation is reached before that the first vehicle access the CA with a settling time T of about 17 [s].

The good performance of the control algorithm is also confirmed by results shown in Fig. 8.13d where the position of both the first and the third vehicle, i.e. $p_1(t)$ and $p_3(t)$, are plotted against the position of the second vehicle, i.e. $p_2(t)$. As it can be observed, both trajectories tangentially touch the critical colliding area, indicated by the red square, while the ideal trajectories (dashed-dotted line), that vehicles would have followed if their initial velocities would have been held without any correction, again uncover the occurrence of collisions without any control. Note that, vertical lines in Fig. 8.13 b)-c) and in Fig. 8.14 a)-b) indicate the time instant at the witch each vehicle enters and exits the CA. Note that the different colors refer to the different vehicles (some of the vertical lines are not visible since they are overlapped).

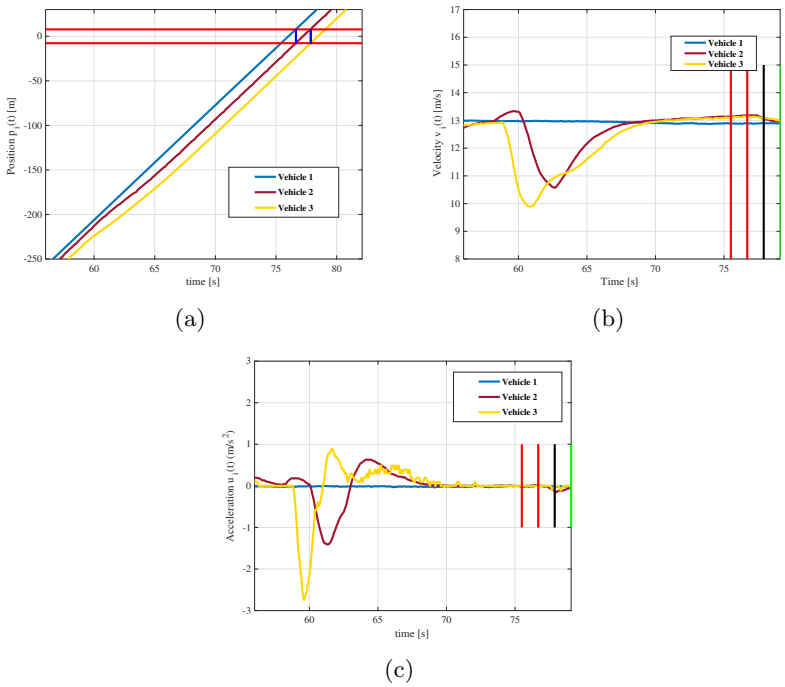


Figure 8.15: Two autonomous vehicles with one human-driven vehicle scenario. Experimental results: a) Time history of vehicles positions (boundaries of the CA: dash-dots horizontal lines). b) Time history of vehicles velocities. c) Time history of vehicles accelerations.

8.3.2 Two autonomous vehicles with one human-driven vehicle scenario

Results related to this road scenario are depicted in Fig. 8.15. Specifically, the time histories of positions, velocities, and accelerations reported respectively in Fig. 8.15a, Fig. 8.15b and Fig. 8.15c, confirm the effectiveness of the proposed control strategy in guaranteeing the exclusive vehicles access into the CA, whose boundaries are indicated with dashed-dotted horizontal lines in Fig. 8.15a. Indeed, only when the human-driven vehicle (the first to access the CA) has exited the CA, the second vehicle is just ready to enter the intersection (as highlighted by the vertical solid line). Finally, note that, according to the theoretical

derivation, the desired inter-vehicle spacing is achieved before that the first vehicle access the CA, hence ensuring collision avoidance at the junction.

8.4 Concluding remarks

In this chapter we have experimentally tested the distributed nonlinear finite-time control algorithm in Chapter 7 that solves the problem of coordinating autonomous vehicles at traffic intersections over $5G$ communication networks. The experimental validation campaign has been carried out at AstaZero test track (near Gothenburg, Sweden) by exploiting three heterogeneous vehicles, properly equipped with specific communication and control hardware: Volvo Car XC90; Volvo Car S90; Volvo Truck FH16.
We have provided details on the vehicles architectures focusing both on hardware devices and software components. Then, we have described the experimental driving scenario. Finally, we have disclosed the experimental results. They have confirmed the effectiveness of the proposed approach in guaranteeing, in real on-the-road scenarios, the safe crossing of autonomous connected vehicles at traffic junctions.

CHAPTER 9

Conclusions

In this thesis the cooperative driving control problem of autonomous connected vehicles has been addressed from networked control systems perspective. We have focused our attention on two open control problem both in cooperative driving application literature and in the general context of networked control systems, namely:

1. designing distributed cooperative control algorithms that are resilient and robust to multiple time-varying communication delays and packet losses;

2. designing resilient secure distributed control algorithms able to counteract different security vulnerabilities when considering the wireless communication network non-ideal.

To address the challenge 1, in this thesis we have proposed in Chapter 4 the novel adaptive distributed cooperative control so to ensuring the cooperative driving despite the presence of communication delays (assumed to be heterogeneous and time-varying) and also external disturbances. The stability of the adaptive strategy and its robustness w.r.t. uncertainties are analytically proven by exploiting the Lyapunov-Krasovskii method and the stability criterion is expressed as an LMI whose solution also provides the estimate of the delay margin that guarantees stability. The effectiveness and robustness of the proposed strategy is shown by using PLEXE simulator and Matlab/Simulink

platform.
Again for addressing the challenge 1, we have also proposed in Chapter 7 a nonlinear finite controller for the specific cooperative driving application of autonomous vehicles approaching the traffic junction. The nonlinear finite time controller has been chosen since in this application a fundamental problem is to guarantee, besides the robustness to communication impairments, that the desired virtual formation is effectively reached before vehicles enter the Conflicting Area. The stability analysis of the control strategy is an on-going work while its effectiveness is validated in numerical and experimental way. Indeed some on the road tests, involving three vehicles properly equipped for autonomous driving, have been carried out at the AstaZero test track near Gothenburg (Sweden). The related experimental results have confirmed the effectiveness of the nonlinear streategy in guaranteeing the safe crossing in real on-the-road scenarios.
For dealing with the challenge 2, we have proposed in Chapter 6 a novel distributed collaborative strategy that guarantees the platoon formation in adversarial environment and that allows to promptly react to security vulnerabilities, such as messages manipulation attacks and communication capability attacks. The proposed distributed control approach also leverages a real-time voting technique to achieve the complete mitigation of some of the most critical effects due to malicious attacks. The stability of the strategy has been demonstrated by exploiting the Lyapunov-Krasovskii theory and an extensive simulation analysis discloses the effectiveness, the robustness and resiliency of the proposed approach and its capabilities in reacting to the malicious attack effects.

9.1 Future Works

Future works of this thesis could include:

- the stability analysis of the nonlinear finite-time controller proposed in Chapter 7;
- the experimental validation of the cooperative driving control strategies proposed in Chapter 4 and Chapter 6;

- theoretical robustness analysis of the adaptive distributed cooperative control (proposed in Chapter 4) not only in presence of external disturbances, but also in presence of parameters uncertainties on vehicles dynamics;
- robustness analysis of the resilient control strategy (proposed in Chapter 6) and of the finite-time nonlinear controller (proposed in Chapter 7) in presence of both external disturbances and vehicle dynamics parameters uncertainties.

Bibliography

[1] `https://www.abdynamics.com/en/products/track-testing/driving-robots/pedal-robots`.

[2] Saneeha Ahmed and Kemal Tepe. Misbehaviour detection in vehicular networks using logistic trust. In *Wireless Communications and Networking Conference (WCNC), 2016 IEEE*, pages 1–6. IEEE, 2016.

[3] Ahmad Al-Dabbagh, Yuzhe Li, and Tongwen Chen. An intrusion detection system for cyber attacks in wireless networked control systems. *IEEE Transactions on Circuits and Systems II: Express Briefs*, 2017.

[4] Mohammed Saeed Al-Kahtani. Survey on security attacks in vehicular ad hoc networks (vanets). In *6th International Conference on Signal Processing and Communication Systems (ICSPCS)*, pages 1–9. IEEE, 2012.

[5] Mahmoud Al-Qutayri, Chan Yeun, and Faisal Al-Hawi. *Security and privacy of intelligent VANETs*. INTECH Open Access Publisher, 2010.

[6] Waleed Alasmary and Weihua Zhuang. Mobility impact in IEEE 802.11 p infrastructureless vehicular networks. *Ad Hoc Networks*, 10(2):222–230, 2012.

[7] Cristina Alcaraz, Javier Lopez, and Stephen Wolthusen. Ocpp protocol: Security threats and challenges. *IEEE Transactions on Smart Grid*, 2017.

[8] Luis Alvarez and Roberto Horowitz. Safe platooning in automated highway systems. *California Partners for Advanced Transit and Highways (PATH)*, 1997.

[9] Luis Alvarez and Roberto Horowitz. Safe platooning in automated highway systems part i: Safety regions design. *Vehicle System Dynamics*, 32(1):23–55, 1999.

[10] Mani Amoozadeh, Hui Deng, Chen-Nee Chuah, H Michael Zhang, and Dipak Ghosal. Platoon management with cooperative adaptive cruise control enabled by vanet. *Vehicular Communications*, 2(2):110–123, 2015.

[11] Mani Amoozadeh, Arun Raghuramu, Chen-Nee Chuah, Dipak Ghosal, H Michael Zhang, Jeff Rowe, and Karl Levitt. Security vulnerabilities of connected vehicle streams and their impact on cooperative driving. *IEEE Communications Magazine*, 53(6):126–132, 2015.

[12] Natalya An, Jens Mittag, and Hannes Hartenstein. Designing fail-safe and traffic efficient 802.11 p-based rear-end collision avoidance. *Ad Hoc Networks*, 37:3–13, 2016.

[13] Mikael Asplund. Poster: Securing vehicular platoon membership. In *IEEE Vehicular Networking Conference*, pages 119–120. IEEE Computer Society, 2014.

[14] TJ Ayres, L Li, D Schleuning, and D Young. Preferred time-headway of highway drivers. In *2001 IEEE Proceedings. on Intelligent Transportation Systems*, pages 826–829. IEEE, 2001.

[15] Bassam Bamieh, Mihailo R Jovanovic, Partha Mitra, and Stacy Patterson. Coherence in large-scale networks: Dimension-dependent limitations of local feedback. *IEEE Transactions on Automatic Control*, 57(9):2235–2249, 2012.

[16] Marcus Bartels and Herbert Werner. Cooperative and consensus-based approaches to formation control of autonomous vehicles. *IFAC Proceedings Volumes*, 47(3):8079–8084, 2014.

[17] L.D. Baskar, B. De Schutter, J. Hellendoorn, and Z. Papp. Traffic control and intelligent vehicle highway systems: a survey. *Intelligent Transport Systems, IET*, 5(1):38–52, March 2011.

[18] Alessandro Bazzi, Barbara M Masini, Alberto Zanella, and Ilaria Thibault. On the performance of ieee 802.11 p and lte-v2v for the cooperative awareness of connected vehicles. *IEEE Transactions on Vehicular Technology*, 66(11):10419–10432, 2017.

[19] Ola Benderius, Christian Berger, and Victor Malmsten Lundgren. The best rated human–machine interface design for autonomous vehicles in the 2016 grand cooperative driving challenge. *IEEE Transactions on Intelligent Transportation Systems*, 19(4):1302–1307, 2018.

[20] Christian Berger. An open continuous deployment infrastructure for a self-driving vehicle ecosystem. In *IFIP International Conference on Open Source Systems*, pages 177–183. Springer, 2016.

[21] Christian Berger, Björnborg Nguyen, and Ola Benderius. Containerized development and microservices for self-driving vehicles: Experiences & best practices. In *Software Architecture Workshops (ICSAW), 2017 IEEE International Conference on*, pages 7–12. IEEE, 2017.

[22] Sanjay P Bhat and Dennis S Bernstein. Finite-time stability of continuous autonomous systems. *SIAM Journal on Control and Optimization*, 38(3):751–766, 2000.

[23] SK Bhavithra, KP Vijayakumar, and P Ganeshkumar. A robust approach for jamming attack detection in vanet.

[24] Sourav Kumar Bhoi and Pabitra Mohan Khilar. Vehicular communication: a survey. *IET Networks*, 3(3):204–217, 2014.

[25] Alessio Botta, Antonio Pescapé, and Giorgio Ventre. Quality of service statistics over heterogeneous networks: Analysis and applications. *European Journal of Operational Research*, 191(3):1075–1088, 2008.

[26] Azzedine Boukerche, Horacio ABF Oliveira, Eduardo F Nakamura, and Antonio AF Loureiro. Vehicular ad hoc networks: A new challenge for localization-based systems. *Computer communications*, 31(12):2838–2849, 2008.

[27] Stephen P Boyd, Laurent El Ghaoui, Eric Feron, and Venkataramanan Balakrishnan. *Linear matrix inequalities in system and control theory*, volume 15. SIAM, 1994.

[28] Corentin Briat. Linear parameter-varying and time-delay systems. *Analysis, Observation, Filtering & Control*, 3, 2014.

[29] Yong-Yan Cao, You-Xian Sun, and Chuwang Cheng. Delay-dependent robust stabilization of uncertain systems with multiple state delays. *Automatic Control, IEEE Transactions on*, 43(11):1608–1612, 1998.

[30] Yongcan Cao, Wenwu Yu, Wei Ren, and Guanrong Chen. An overview of recent progress in the study of distributed multi-agent coordination. *IEEE Transactions on Industrial informatics*, 9(1):427–438, 2013.

[31] Derek Caveney and William B Dunbar. Cooperative driving: beyond v2v as an adas sensor. In *Intelligent Vehicles Symposium (IV), 2012 IEEE*, pages 529–534. IEEE, 2012.

[32] Gang Chen and Frank L Lewis. Leader-following control for multiple inertial agents. *International Journal of Robust and Nonlinear Control*, 21(8):925–942, 2011.

[33] Jinran Chen, Shubha Kher, and Arun Somani. Distributed fault detection of wireless sensor networks. In *Proceedings of the 2006 workshop on Dependability issues in wireless ad hoc networks and sensor networks*, pages 65–72. ACM, 2006.

[34] Lei Chen and Cristofer Englund. Cooperative intersection management: a survey. *IEEE Transactions on Intelligent Transportation Systems*, 17(2):570–586, 2016.

[35] Shanzhi Chen, Jinling Hu, Yan Shi, Ying Peng, Jiayi Fang, Rui Zhao, and Li Zhao. Vehicle-to-everything (v2x) services supported by lte-based systems and 5g. *IEEE Communications Standards Magazine*, 1(2):70–76, 2017.

[36] Rutger Claes and Tom Holvoet. Traffic coordination using aggregation-based traffic predictions. *IEEE Intelligent Systems*, 29(4):96–100, 2014.

[37] Rutger Claes, Tom Holvoet, and Danny Weyns. A decentralized approach for anticipatory vehicle routing using delegate multiagent systems. *IEEE Transactions on Intelligent Transportation Systems*, 12(2):364–373, 2011.

[38] Erik Coelingh and Stefan Solyom. All aboard the robotic road train. *IEEE Spectrum*, 49(11):34–39, 2012.

[39] Claude Crepeau, Carlton R Davis, and Muthucumaru Maheswaran. A secure manet routing protocol with resilience against byzantine behaviours of malicious or selfish nodes. In *Advanced Information Networking and Applications Workshops, 2007, AINAW'07. 21st International Conference on*, volume 2, pages 19–26. IEEE, 2007.

[40] Soodeh Dadras, Ryan M Gerdes, and Rajnikant Sharma. Vehicular platooning in an adversarial environment. In *Proceedings of the 10th ACM Symposium on Information, Computer and Communications Security*, pages 167–178. ACM, 2015.

[41] Swaroop Darbha and KR Rajagopal. Intelligent cruise control systems and traffic flow stability. *Transportation Research Part C: Emerging Technologies*, 7(6):329–352, 1999.

[42] John M Davis, Ian A Gravagne, Robert J Marks, and Alice A Ramos. Algebraic and dynamic lyapunov equations on time scales. In *System Theory (SSST), 2010 42nd Southeastern Symposium on*, pages 329–334. IEEE, 2010.

[43] Gabriel Rodrigues de Campos, Paolo Falcone, Robert Hult, Henk Wymeersch, and Jonas Sjöberg. Traffic coordination at road intersections: Autonomous decision-making algorithms using model-based heuristics. *IEEE Intelligent Transportation Systems Magazine*, 9(1):8–21, 2017.

[44] Bruce DeBruhl, Sean Weerakkody, Bruno Sinopoli, and Patrick Tague. Is your commute driving you crazy?: a study of misbehavior in vehicular platoons. In *Proceedings of the 8th ACM Conference on Security & Privacy in Wireless and Mobile Networks*, page 22. ACM, 2015.

[45] K. C. Dey, L. Yan, X. Wang, Y. Wang, H. Shen, M. Chowdhury, L. Yu, C. Qiu, and V. Soundararaj. A review of communication, driver characteristics, and controls aspects of cooperative adaptive cruise control (cacc). *IEEE Transactions on Intelligent Transportation Systems*, 17(2):491–509, 2016.

[46] Kakan C Dey, Li Yan, Xujie Wang, Yue Wang, Haiying Shen, Mashrur Chowdhury, Lei Yu, Chenxi Qiu, and Vivekgautham Soundararaj. A review of communication, driver characteristics, and controls aspects of cooperative adaptive cruise control (cacc). *IEEE Transactions on Intelligent Transportation Systems*, 17(2):491–509, 2016.

[47] Sanjay K Dhurandher, Mohammad S Obaidat, Amrit Jaiswal, Akanksha Tiwari, and Ankur Tyagi. Vehicular security through reputation and plausibility checks. *IEEE Systems Journal*, 8(2):384–394, 2014.

[48] Marco Di Vaio, Alberto Petrillo, and Stefania Santini. On the robustness of a distributed adaptive synchronization protocol for connected autonomous vehicles with multiple disturbances and communication delays. In *2018 IEEE 57th Conference on Decision and Control (CDC), To appear.*

[49] João AFF Dias, Joel JPC Rodrigues, and Liang Zhou. Cooperation advances on vehicular communications: A survey. *Vehicular communications*, 1(1):22–32, 2014.

[50] Derui Ding, Qing-Long Han, Yang Xiang, Xiaohua Ge, and Xian-Ming Zhang. A survey on security control and attack detection for industrial cyber-physical systems. *Neurocomputing*, 275:1674–1683, 2018.

[51] Florian Dorfler and Francesco Bullo. Synchronization and transient stability in power networks and nonuniform kuramoto oscillators. *SIAM Journal on Control and Optimization*, 50(3):1616–1642, 2012.

[52] Florian Dotzer, Lars Fischer, and Przemyslaw Magiera. Vars: A vehicle ad-hoc network reputation system. In *World of Wireless Mobile and Multimedia Networks, 2005. WoWMoM 2005. Sixth IEEE International Symposium on a*, pages 454–456. IEEE, 2005.

[53] SS Dragomir, J Pecaric, and LE Persson. Some inequalities of hadamard type. *Soochow J. Math*, 21(3):335–341, 1995.

[54] dSpace. https://www.dspace.com. Online Available.

[55] Guang-Ren Duan and Ron J Patton. A note on hurwitz stability of matrices. *Automatica*, 34(4):509–511, 1998.

[56] Richard Gilles Engoulou, Martine Bellaïche, Samuel Pierre, and Alejandro Quintero. Vanet security surveys. *Computer Communications*, 44:1–13, 2014.

[57] Haneen Farah and Haris N Koutsopoulos. Do cooperative systems make driversâ€™ car-following behavior safer? *Transportation research part C: emerging technologies*, 41:61–72, 2014.

[58] David G. Feingold and Richard S. Varga. Block diagonally dominant matrices and generalizations of the Gerschgorin circle theorem. *Pacific J. Math*, 12(4):1241–1250, 1962.

[59] P. Fernandes and U. Nunes. Multiplatooning leaders positioning and cooperative behavior algorithms of communicant automated vehicles for high traffic capacity. *IEEE Transactions on Intelligent Transportation Systems*, 16(3):1172–1187, 2015.

[60] Giovanni Fiengo, Alberto Petrillo, Alessandro Salvi, Stefania Santini, and Manuela Tufo. A control strategy for reducing traffic waves in delayed vehicular networks. In *Decision and Control (CDC), 2016 IEEE 55th Conference on*, pages 2462–2467. IEEE, 2016.

[61] L. Figueiredo, I. Jesus, J.A.T. Machado, J.R. Ferreira, and J.L.M. de Carvalho. Towards the development of intelligent transportation systems. In *Intelligent Transportation Systems, 2001. Proceedings. 2001 IEEE*, pages 1206–1211, 2001.

[62] Emilia Fridman. *Introduction to time-delay systems: Analysis and control*. Springer, 2014.

[63] Emilia Fridman and Yury Orlov. Exponential stability of linear distributed parameter systems with time-varying delays. *Automatica*, 45(1):194–201, 2009.

[64] Emilia Fridman and Uri Shaked. Delay-dependent stability and H_∞ control: constant and time-varying delays. *International Journal of Control*, 76(1):48–60, 2003.

[65] Emilia Fridman, Uri Shaked, and Vladimir Suplin. Input/output delay approach to robust sampled-data h_∞ control. *Systems & Control Letters*, 54(3):271–282, 2005.

[66] Feng Gao, Shengbo Eben Li, Yang Zheng, and Dongsuk Kum. Robust control of heterogeneous vehicular platoon with uncertain dynamics and communication delay. *IET Intelligent Transport Systems*, 10(7):503–513, 2016.

[67] Mevlut Turker Garip, Mehmet Emre Gursoy, Peter Reiher, and Mario Gerla. Congestion attacks to autonomous cars using vehicular botnets. In *NDSS Workshop on Security of Emerging Networking Technologies (SENT), San Diego, CA*, 2015.

[68] Xiaohua Ge, Fuwen Yang, and Qing-Long Han. Distributed networked control systems: A brief overview. *Information Sciences*, 380:117–131, 2017.

[69] Christopher David Godsil, Gordon Royle, and CD Godsil. *Algebraic graph theory*, volume 207. Springer New York, 2001.

[70] Jian Gong, Yuan Zhao, and Zibao Lu. Finite-time bidirectional platoon control of interconnected vehicles with multiple disturbances. In *Control Conference (CCC), 2017 36th Chinese*, pages 9472–9477. IEEE, 2017.

[71] Jyoti Grover, Manoj Singh Gaur, and Vijay Laxmi. Trust establishment techniques in vanet. In *Wireless Networks and Security*, pages 273–301. Springer, 2013.

[72] K. Gu, V.L. Kharitonov, and J. Chen. *Stability of Time-Delay Systems*. Control Engineering. Birkhäuser Boston, 2012.

[73] Keqin Gu, Jie Chen, and Vladimir L Kharitonov. *Stability of time-delay systems*. Springer Science & Business Media, 2003.

[74] Keqin Gu and Silviu-Iulian Niculescu. Survey on recent results in the stability and control of time-delay systems*. *Journal of Dynamic Systems, Measurement, and Control*, 125(2):158–165, 2003.

[75] Xinping Guan, Bo Yang, Cailian Chen, Wenbin Dai, and Yiyin Wang. A comprehensive overview of cyber-physical systems: from perspective of feedback system. *IEEE/CAA Journal of Automatica Sinica*, 3(1):1–14, 2016.

[76] Ge Guo and Wei Yue. Autonomous platoon control allowing range-limited sensors. *IEEE Transactions on Vehicular Technology*, 61(7):2901–2912, 2012.

[77] Xianggui Guo, Jianliang Wang, Fang Liao, and Rodney Swee Huat Teo. Distributed adaptive integrated-sliding-mode controller synthesis for string stability of vehicle platoons. *IEEE Transactions on Intelligent Transportation Systems*, 17(9):2419–2429, 2016.

[78] Jason J Haas. The effects of wireless jamming on vehicle platooning, 2009.

[79] Michael Haddrell. Towards an autonomous vehicle enabled society: cyber attacks and countermeasures.

[80] Qing-Long Han and Keqin Gu. Stability of Linear Systems With Time-Varying Delay: a Generalized Discretized Lyapunov Functional Approach. *Asian Journal of Control*, 3(3):170–180, 2001.

[81] He Hao and Prabir Barooah. Stability and Robustness of Large Platoons of Vehicles with Double-integrator Models and Nearest Neighbor Interaction. *International Journal of Robust and Nonlinear Control*, pages 1099 – 1125, 2012.

[82] He Hao, Prabir Barooah, and Prashant G Mehta. Stability margin scaling laws for distributed formation control as a function of network structure. *IEEE Transactions on Automatic Control*, 56(4):923–929, 2011.

[83] H. Hartenstein and K. Laberteaux. *VANET Vehicular Applications and Inter-Networking Technologies*. Intelligent Transport Systems. Wiley, 2009.

[84] Hamssa Hasrouny, Abed Ellatif Samhat, Carole Bassil, and Anis Laouiti. Vanet security challenges and solutions: A survey. *Vehicular Communications*, 2017.

[85] Li He and Wen Tao Zhu. Mitigating dos attacks against signature-based authentication in vanets. In *Computer Science and Automation Engineering (CSAE), 2012 IEEE International Conference on*, volume 3, pages 261–265. IEEE, 2012.

[86] K. Hengster-Movric. Synchronizing region approach to identical lti system state synchronization distributed control. In *20th International Conference on Process Control (PC)*, pages 54–59, June 2015.

[87] Kristian Hengster-Movric, Frank L Lewis, Michael Šebek, and Tomáš Vyhlídal. Cooperative synchronization control for agents with control delays: A synchronizing region approach. *Journal of the Franklin Institute*, 352(5):2002–2028, 2015.

[88] R. A. Horn and C. R. Johnson. *Matrix Analisis*. University Press, Cambridge, 1987.

[89] Roger A Horn and Charles R Johnson. *Matrix analysis*. Cambridge university press, 2012.

[90] Wenying Hou, Min Yue Fu, and Huanshui Zhang. Consensusability of linear multi-agent systems with time delay. *International Journal of Robust and Nonlinear Control*, 26(12):2529–2541, 2016.

[91] Wenying Hou, Minyue Fu, Huanshui Zhang, and Zongze Wu. Consensus conditions for general second-order multi-agent systems with communication delay. *Automatica*, 75:293–298, 2017.

[92] Robert Hult, Feyyaz Emre Sancar, Mehdi Jalalmaad, Arun Vijayan, Albin Severinson, Marco Di Vaio, Paolo Falcone, Baris Fidan, and Stefania; Santini. Design and experimental validation of a cooperative driving control architecture for the grand cooperative driving challenge 2016. *Transactions on Intelligent Transportation Systems*, 2017,to appear in October.

[93] Robert Hult, Mario Zanon, Sébastien Gros, and Paolo Falcone. Primal decomposition of the optimal coordination of vehicles at traffic intersections. In *Decision and Control (CDC), 2016 IEEE 55th Conference on*, pages 2567–2573. IEEE, 2016.

[94] Jesús Téllez Isaac, Sherali Zeadally, and José Sierra Camara. Security attacks and solutions for vehicular ad hoc networks. *IET Communications*, 4(7):894–903, 2010.

[95] Morten Bornø Jensen, Mark Philip Philipsen, Andreas Møgelmose, Thomas Baltzer Moeslund, and Mohan Manubhai Trivedi. Vision for looking at traffic lights: Issues, survey, and perspectives. *IEEE Transactions on Intelligent Transportation Systems*, 17(7):1800–1815, 2016.

[96] Dongyao Jia, Kejie Lu, Jianping Wang, Xiang Zhang, and Xuemin Shen. A survey on platoon-based vehicular cyber-physical systems. *IEEE communications surveys & tutorials*, 18(1):263–284, 2016.

[97] Dongyao Jia and Dong Ngoduy. Platoon based cooperative driving model with consideration of realistic inter-vehicle communication. *Transportation Research Part C: Emerging Technologies*, 68:245–264, 2016.

[98] I Ge Jin and Gábor Orosz. Dynamics of connected vehicle systems with delayed acceleration feedback. *Transportation Research Part C: Emerging Technologies*, 46:46–64, 2014.

[99] Md Abdus Samad Kamal, Jun-ichi Imura, Tomohisa Hayakawa, Akira Ohata, and Kazuyuki Aihara. A vehicle-intersection coordination scheme for smooth flows of traffic without using traffic lights. *IEEE Transactions on Intelligent Transportation Systems*, 16(3):1136–1147, 2015.

[100] Chung-Yao Kaoa and Bo Lincolnb. Simple stability criteria for systems with time-varying delays. *Automatica*, 40:1429–1434, 2004.

[101] R. P. Karrer, I. Matyasovszki, A. Botta, and A. Pescapé. Magnets - experiences from deploying a joint research-operational next-generation wireless access network testbed. In *2007 3rd International Conference on Testbeds and Research Infrastructure for the Development of Networks and Communities*, pages 1–10, May 2007.

[102] Roger P Karrer, Istvan Matyasovszki, Alessio Botta, and Antonio Pescapé. Experimental evaluation and characterization of the magnets wireless backbone. In *Proceedings of the 1st international workshop on Wireless network testbeds, experimental evaluation & characterization*, pages 26–33. ACM, 2006.

[103] Chaker Abdelaziz Kerrache, Nasreddine Lagraa, Carlos T Calafate, Juan-Carlos Cano, and Pietro Manzoni. T-vnets: A novel trust architecture for vehicular networks using the standardized messaging services of etsi its. *Computer Communications*, 93:68–83, 2016.

[104] Hassan K Khalil. Noninear systems. *Prentice-Hall, New Jersey*, 2(5):5–1, 1996.

[105] Vladimir L. Kharitonov and S. I. Niculescu. On the stability of linear systems with uncertain delay. *IEEE Transactions on Automatic Control*, 48(1):127–132, 2003.

[106] Roozbeh Kianfar, Bruno Augusto, Alireza Ebadighajari, Usman Hakeem, Josef Nilsson, Ali Raza, Reza S Tabar, Naga VishnuKanth Irukulapati, Cristofer Englund, Paolo Falcone, et al. Design and

experimental validation of a cooperative driving system in the grand cooperative driving challenge. *IEEE Transactions on Intelligent Transportation Systems*, 13(3):994–1007, 2012.

[107] Roozbeh Kianfar, Paolo Falcone, and Jonas Fredriksson. A control matching model predictive control approach to string stable vehicle platooning. *Control Engineering Practice*, 45:163–173, 2015.

[108] Jin-Hoon Kim. Delay and its time-derivative dependent robust stability of time-delayed linear systems with uncertainty. *IEEE Transactions on Automatic Control*, 46(5):789–792, 2001.

[109] Yeongkwun Kim and Injoo Kim. Security issues in vehicular networks. In *2013 International Conference on Information Networking (ICOIN)*, pages 468–472. IEEE, 2013.

[110] Neeraj Kumar and Naveen Chilamkurti. Collaborative trust aware intelligent intrusion detection in vanets. *Computers & Electrical Engineering*, 40(6):1981–1996, 2014.

[111] Clark Letter and Lily Elefteriadou. Efficient control of fully automated connected vehicles at freeway merge segments. *Transportation Research Part C: Emerging Technologies*, 80:190–205, 2017.

[112] Chunguang Li and Guanrong Chen. Synchronization in general complex dynamical networks with coupling delays. *Physica A: Statistical Mechanics and its Applications*, 343:263–278, 2004.

[113] Li Li and Fei-Yue Wang. Cooperative driving at blind crossings using intervehicle communication. *Vehicular Technology, IEEE Transactions on*, 55(6):1712–1724, 2006.

[114] Li Li, Ding Wen, and Danya Yao. A survey of traffic control with vehicular communications. *IEEE Transactions on Intelligent Transportation Systems*, 15(1):425–432, 2014.

[115] Shengbo Eben Li, Yang Zheng, Keqiang Li, and Jianqiang Wang. An overview of vehicular platoon control under the four-component framework. In *Intelligent Vehicles Symposium (IV), 2015 IEEE*, pages 286–291. IEEE, 2015.

[116] Shengbo Eben Li, Yang Zheng, Keqiang Li, Le-Yi Wang, and Hongwei Zhang. Platoon control of connected vehicles from a networked control perspective: Literature review, component modeling, and controller synthesis. *IEEE Transactions on Vehicular Technology*, 2017.

[117] Xi Li and Carlos E De Souza. Criteria for robust stability and stabilization of uncertain linear systems with state delay. *Automatica*, 33(9):1657–1662, 1997.

[118] Zhongkui Li, Zhisheng Duan, Guanrong Chen, and Lin Huang. Consensus of multiagent systems and synchronization of complex networks: a unified viewpoint. *IEEE Transactions on Circuits and Systems I: Regular Papers*, 57(1):213–224, 2010.

[119] Zhongkui Li, Guanghui Wen, Zhisheng Duan, and Wei Ren. Designing fully distributed consensus protocols for linear multi-agent systems with directed graphs. *IEEE Transactions on Automatic Control*, 60(4):1152–1157, 2015.

[120] Fu Lin, Makan Fardad, and Mihailo R Jovanovic. Optimal control of vehicular formations with nearest neighbor interactions. *IEEE Transactions on Automatic Control*, 57(9):2203–2218, 2012.

[121] Xiaodong Lin, Rongxing Lu, Chenxi Zhang, Haojin Zhu, Pin-Han Ho, and Xuemin Shen. Security in vehicular ad hoc networks. *Communications Magazine, IEEE*, 46(4):88–95, 2008.

[122] Jennie Lioris, Ramtin Pedarsani, Fatma Yildiz Tascikaraoglu, and Pravin Varaiya. Platoons of connected vehicles can double throughput in urban roads. *Transportation Research Part C: Emerging Technologies*, 77:292–305, 2017.

[123] Cheng-Lin Liu, Lihua Xie, Shuai Liu, and Fei Liu. Asynchronously compensated synchronization algorithm for multiple harmonic oscillators with communication delay. *International Journal of Robust and Nonlinear Control*, 27(2):281–297, 2017.

[124] Jiafa Liu, Di Ma, André Weimerskirch, and Haojin Zhu. Secure and safe automated vehicle platooning. *IEEE Reliability Magazine, Special Issue on IoT Security*, 2016.

[125] Keng-Hao Liu, Po-Fu Wu, Yu-Shen Tsai, Andy An-Kai Jeng, and Kang Li. Improved braking control of the cooperative adaptive cruise control system in low speed traffic conditions. In *82nd IEEE Vehicular Technology Conference (VTC Fall)*, pages 1–2. IEEE, 2015.

[126] Peng Liu, Umit Ozguner, and Yeqing Zhang. Distributed mpc for cooperative highway driving and energy-economy validation via microscopic simulations. *Transportation Research Part C: Emerging Technologies*, 77:80–95, 2017.

[127] Yonggui Liu, Bugong Xu, and Yuehua Ding. Convergence analysis of cooperative braking control for interconnected vehicle systems. *IEEE Transactions on Intelligent Transportation Systems*, 18(7):1894–1906, 2017.

[128] Johan Lofberg. Yalmip: A toolbox for modeling and optimization in matlab. In *Computer Aided Control Systems Design, 2004 IEEE International Symposium on*, pages 284–289. IEEE, 2004.

[129] Xiaoqing Lu, Renquan Lu, Shihua Chen, and Jinhu Lu. Finite-time distributed tracking control for multi-agent systems with a virtual leader. *IEEE Transactions on Circuits and Systems I: Regular Papers*, 60(2):352–362, 2013.

[130] Santa Maiti, Stephan Winter, and Lars Kulik. A conceptualization of vehicle platoons and platoon operations. *Transportation Research Part C: Emerging Technologies*, 80:1–19, 2017.

[131] Jan P Maschuw and Dirk Abel. Longitudinal vehicle guidance in networks with changing communication topology. *IFAC Proceedings Volumes*, 43(7):785–790, 2010.

[132] Alejandro Ivan Morales Medina, Nathan van de Wouw, and Henk Nijmeijer. Cooperative intersection control based on virtual platooning. *IEEE Transactions on Intelligent Transportation Systems*, 2017.

[133] D Mehdi, EK Boukas, and Zi-Kuan Liu. Dynamical systems with multiple time-varying delays: Stability and stabilizability. *Journal of optimization theory and applications*, 113(3):537–565, 2002.

[134] Mohamed Nidhal Mejri, Jalel Ben-Othman, and Mohamed Hamdi. Survey on vanet security challenges and possible cryptographic solutions. *Vehicular Communications*, 1(2):53–66, 2014.

[135] Ziyang Meng, Zhongkui Li, Athanasios V Vasilakos, and Shiming Chen. Delay-induced synchronization of identical linear multiagent systems. *IEEE Transactions on Cybernetics*, 43(2):476–489, 2013.

[136] Vicente Milanés, Steven E Shladover, John Spring, Christopher Nowakowski, Hiroshi Kawazoe, and Masahide Nakamura. Cooperative adaptive cruise control in real traffic situations. *IEEE Transactions on Intelligent Transportation Systems*, 15(1):296–305, 2014.

[137] Aikaterini Mitrokotsa and Christos Dimitrakakis. Intrusion detection in manet using classification algorithms: The effects of cost and model selection. *Ad Hoc Networks*, 11(1):226–237, 2013.

[138] Seungwuk Moon, Ilki Moon, and Kyongsu Yi. Design, tuning, and evaluation of a full-range adaptive cruise control system with collision avoidance. *Control Engineering Practice*, 17(4):442–455, 2009.

[139] Carlos Murguia, Rob HB Fey, and Henk Nijmeijer. Synchronization of identical linear systems and diffusive time-delayed couplings. *IEEE Transactions on Circuits and Systems I: Regular Papers*, 61(6):1801–1814, 2014.

[140] Richard M Murray. Recent research in cooperative control of multivehicle systems. *Journal of Dynamic Systems, Measurement, and Control*, 129(5):571–583, 2007.

[141] Mostofa Kamal Nasir, ASM Delowar Hossain, Md Sazzad Hossain, Md Mosaddik Hasan, and Md Belayet Ali. Security challenges and implementation mechanism for vehicular ad hoc network. *International Journal Of Scientific & Technology Research*, 2(4):156–161, 2013.

[142] Tuan Anh Nguyen, Doina Bucur, Marco Aiello, and Kenji Tei. Applying time series analysis and neighbourhood voting in a decentralised approach for fault detection and classification in wsns.

In *Proceedings of the Fourth Symposium on Information and Communication Technology*, pages 234–241. ACM, 2013.

[143] Reza Olfati-Saber, J. Alex Fax, and Richard Murray. Consensus and Cooperation in Networked Multi-Agent System. In *Proceedings of the IEEE*, volume 95, pages 215–233, January 2007.

[144] Reza Olfati-Saber and Richard M Murray. Consensus problems in networks of agents with switching topology and time-delays. *Automatic Control, IEEE Transactions on*, 49(9):1520–1533, 2004.

[145] World Health Organization. *Global status report on road safety 2015*. World Health Organization, 2015.

[146] Antonis Papachristodoulou, Ali Jadbabaie, and Ulrich Munz. Effects of delay in multi-agent consensus and oscillator synchronization. *IEEE Transactions on Automatic Control*, 55(6):1471–1477, 2010.

[147] P. Papadimitratos, A. La Fortelle, K. Evenssen, R. Brignolo, and S. Cosenza. Vehicular communication systems: Enabling technologies, applications, and future outlook on intelligent transportation. *Communications Magazine, IEEE*, 47(11):84–95, November 2009.

[148] Al-Sakib Khan Pathan. *Security of self-organizing networks: MANET, WSN, WMN, VANET*. CRC press, 2016.

[149] Sandhya Peddabachigari, Ajith Abraham, Crina Grosan, and Johnson Thomas. Modeling intrusion detection system using hybrid intelligent systems. *Journal of network and computer applications*, 30(1):114–132, 2007.

[150] Andrés A Peters, Richard H Middleton, and Oliver Mason. Leader tracking in homogeneous vehicle platoons with broadcast delays. *Automatica*, 50(1):64–74, 2014.

[151] Alberto Petrillo, Antonio Pescapé, and Stefania Santini. A collaborative control strategy for platoons of autonomous vehicles in the presence of message falsification attacks. In *Models and Technologies for Intelligent Transportation Systems (MT-ITS), 2017 5th IEEE International Conference on*, pages 110–115. IEEE, 2017.

[152] Alberto Petrillo, Antonio Pescapé, and Stefania Santini. A collaborative approach for improving the security of vehicular scenarios: The case of platooning. *Computer Communications*, 122:59–75, 2018.

[153] Alberto Petrillo, Alessandro Salvi, Stefania Santini, and Antonio Saverio Valente. Adaptive synchronization of linear multi-agent systems with time-varying multiple delays. *Journal of the Franklin Institute*, 354(18):8586–8605, 2017.

[154] Alberto Petrillo, Alessandro Salvi, Stefania Santini, and Antonio Saverio Valente. Adaptive synchronization of linear multi-agent systems with time-varying multiple delays. *Journal of the Franklin Institute*, 2017.

[155] Alberto Petrillo, Alessandro Salvi, Stefania Santini, and Antonio Saverio Valente. Adaptive multi-agents synchronization for collaborative driving of autonomous vehicles with multiple communication delays. *Transportation Research Part C: Emerging Technologies*, 86:372–392, 2018.

[156] Jeroen Ploeg, Dipan P Shukla, Nathan van de Wouw, and Henk Nijmeijer. Controller synthesis for string stability of vehicle platoons. *IEEE Trans. Intelligent Transportation Systems*, 15(2):854–865, 2014.

[157] Michael Quinlan, Tsz-Chiu Au, Jesse Zhu, Nicolae Stiurca, and Peter Stone. Bringing simulation to life: A mixed reality autonomous intersection. In *Intelligent Robots and Systems (IROS), 2010 IEEE/RSJ International Conference on*, pages 6083–6088. IEEE, 2010.

[158] Rajesh Rajamani. *Vehicle dynamics and control*. Springer Science & Business Media, 2011.

[159] Maxim Raya and Jean-Pierre Hubaux. Security aspects of inter-vehicle communications. In *5th Swiss Transport Research Conference (STRC)*, number LCA-CONF-2005-012, 2005.

[160] Maxim Raya and Jean-Pierre Hubaux. Securing vehicular ad hoc networks. *Journal of Computer Security*, 15(1):39–68, 2007.

[161] Maxim Raya, Panagiotis Papadimitratos, Virgil D Gligor, and J-P Hubaux. On data-centric trust establishment in ephemeral ad hoc networks. In *INFOCOM 2008. The 27th Conference on Computer Communications. IEEE*, pages 1238–1246. IEEE, 2008.

[162] Wei Ren and Randal W Beard. *Distributed consensus in multi-vehicle cooperative control*. Springer, 2008.

[163] Wei Ren and Yongcan Cao. *Distributed coordination of multi-agent networks: emergent problems, models, and issues*. Springer Science & Business Media, 2010.

[164] Jean-Pierre Richard. Time-delay systems: an overview of some recent advances and open problems. *Automatica*, 39(10):1667–1694, 2003.

[165] Jackeline Rios-Torres and Andreas A Malikopoulos. A survey on the coordination of connected and automated vehicles at intersections and merging at highway on-ramps. *IEEE Transactions on Intelligent Transportation Systems*, 18(5):1066–1077, 2017.

[166] Paul Rodriguez, Alvaro Luna, Ignacio Candela, Ramon Mujal, Remus Teodorescu, and Frede Blaabjerg. Multiresonant frequency-locked loop for grid synchronization of power converters under distorted grid conditions. *IEEE Transactions on Industrial Electronics*, 58(1):127–138, 2011.

[167] Alessandro Salvi, Stefania Santini, and Antonio Saverio Valente. Design, analysis and performance evaluation of a third order distributed protocol for platooning in the presence of time-varying delays and switching topologies. *Transportation Research Part C: Emerging Technologies*, 80:360–383, 2017.

[168] Feyyaz Emre Sancar, Baris Fidan, Jan P Huissoon, and Steven L Waslander. Mpc based collaborative adaptive cruise control with rear end collision avoidance. In *Intelligent Vehicles Symposium Proceedings, 2014 IEEE*, pages 516–521. IEEE, 2014.

[169] S Santini, A Salvi, AS Valente, A Pescape, M Segata, and R Lo Cigno. A consensus-based approach for platooning with inter-vehicular communications. In *2015 IEEE Conference on Computer Communications (INFOCOM)*, pages 1158–1166. IEEE, 2015.

[170] Stefania Santini, Alessandro Salvi, Antonio Saverio Valente, Antonio Pescapé, Michele Segata, and Renato Lo Cigno. A consensus-based approach for platooning with intervehicular communications and its validation in realistic scenarios. *IEEE Transactions on Vehicular Technology*, 66(3):1985–1999, 2017.

[171] Hichem Sedjelmaci and Sidi Mohammed Senouci. An accurate and efficient collaborative intrusion detection framework to secure vehicular networks. *Computers & Electrical Engineering*, 43:33–47, 2015.

[172] Michele Segata, Stefan Joerer, Bastian Bloessl, Christoph Sommer, Falko Dressler, and Renate Lo Cigno. Plexe: A platooning extension for veins. In *Vehicular Networking Conference (VNC), 2014 IEEE*, pages 53–60. IEEE, 2014.

[173] Anton Selivanov, Alexander Fradkov, and Emilia Fridman. Passification-based decentralized adaptive synchronization of dynamical networks with time-varying delays. *Journal of the Franklin Institute*, 352(1):52–72, 2015.

[174] Georg S Seyboth, Wei Ren, and Frank Allgöwer. Cooperative control of linear multi-agent systems via distributed output regulation and transient synchronization. *Automatica*, 68:132–139, 2016.

[175] Shahaboddin Shamshirband, Nor Badrul Anuar, Miss Laiha Mat Kiah, and Ahmed Patel. An appraisal and design of a multi-agent system based cooperative wireless intrusion detection computational intelligence technique. *Engineering Applications of Artificial Intelligence*, 26(9):2105–2127, 2013.

[176] Elaine Shaw and J Karl Hedrick. String stability analysis for heterogeneous vehicle strings. In *American Control Conference, 2007. ACC'07*, pages 3118–3125. IEEE, 2007.

[177] Lin Shi, Hong Zhu, Shouming Zhong, Yong Zeng, and Jun Cheng. Synchronization for time-varying complex networks based on control. *Journal of Computational and Applied Mathematics*, 301:178–187, 2016.

[178] Mohammad Shokrolah Shirazi and Brendan Tran Morris. Looking at intersections: a survey of intersection monitoring, behavior and safety analysis of recent studies. *IEEE Transactions on Intelligent Transportation Systems*, 18(1):4–24, 2017.

[179] S.E. Shladover. Path at 20 history and major milestones. *Intelligent Transportation Systems, IEEE Transactions on*, 8(4):584–592, Dec 2007.

[180] Christoph Sommer, Reinhard German, and Falko Dressler. Bidirectionally coupled network and road traffic simulation for improved ivc analysis. *IEEE Transactions on Mobile Computing*, 10(1):3–15, 2011.

[181] Philipp Sommer and Roger Wattenhofer. Gradient clock synchronization in wireless sensor networks. In *Proceedings of the 2009 International Conference on Information Processing in Sensor Networks*, IPSN '09, pages 37–48, Washington, DC, USA, 2009. IEEE Computer Society.

[182] Qiang Song, Wenwu Yu, Jinde Cao, and Fang Liu. Reaching synchronization in networked harmonic oscillators with outdated position data. *IEEE transactions on Cybernetics*, 46(7):1566–1578, 2016.

[183] Steven H Strogatz. Exploring complex networks. *Nature*, 410(6825):268–276, 2001.

[184] Karl R Stromberg. *An introduction to classical real analysis*, volume 376. American Mathematical Soc., 2015.

[185] D Swaroop and JK Hedrick. String stability of interconnected systems. *Automatic Control, IEEE Transactions on*, 41(3):349–357, 1996.

[186] DVAHG Swaroop and JK Hedrick. Constant spacing strategies for platooning in automated highway systems. *Journal of dynamic systems, measurement, and control*, 121(3):462–470, 1999.

[187] Sasayuki Tsugawa, Shin Kato, Takeshi Matsui, Hiroshi Naganawa, and H Fujii. An architecture for cooperative driving of automated vehicles. In *Intelligent Transportation Systems, 2000. Proceedings. 2000 IEEE*, pages 422–427. IEEE, 2000.

[188] A. Uno, T. Sakaguchi, and S. Tsugawa. A merging control algorithm based on inter-vehicle communication. In *Proceedings 199 IEEE/IEEJ/JSAI International Conference on Intelligent Transportation Systems (Cat. No.99TH8383)*, pages 783–787, 1999.

[189] Remco Van Der Hofstad. Random graphs and complex networks. *Available on http://www. win. tue. nl/rhofstad/NotesRGCN. pdf*, 2009.

[190] Ruben Visser, Ir CJG van Driel, Ir HH Versteegt, and City Enschede. Co-operative driving on highways, 2005.

[191] Nianfeng Wan, Ardalan Vahidi, and Andre Luckow. Optimal speed advisory for connected vehicles in arterial roads and the impact on mixed traffic. *Transportation Research Part C: Emerging Technologies*, 69:548 – 563, 2016.

[192] Jingyao Wang, Zhisheng Duan, Guanghui Wen, and Guanrong Chen. Distributed robust control of uncertain linear multi-agent systems. *International Journal of Robust and Nonlinear Control*, 25(13):2162–2179, 2015.

[193] Tianbo Wang, Wuneng Zhou, and Shouwei Zhao. Robust synchronization for stochastic delayed complex networks with switching topology and unmodeled dynamics via adaptive control approach. *Communications in Nonlinear Science and Numerical Simulation*, 18(8):2097–2106, 2013.

[194] Lambert Wanninger. Introduction to network rtk. *IAG Working Group*, 4(1):2003–2007, 2004.

[195] Jia Wu, Florent Perronnet, and Abdeljalil Abbas-Turki. Cooperative vehicle-actuator system: a sequence-based framework of cooperative intersections management. *IET Intelligent Transport Systems*, 8(4):352–360, 2013.

[196] Weigang Wu, Jiebin Zhang, Aoxue Luo, and Jiannong Cao. Distributed mutual exclusion algorithms for intersection traffic control. *IEEE Transactions on Parallel and Distributed Systems*, 26(1):65–74, 2015.

[197] Yujia Wu, Shengbo Eben Li, Yang Zheng, and J Karl Hedrick. Distributed sliding mode control for multi-vehicle systems with positive definite topologies. In *2016 IEEE 55th Conference on Decision and Control (CDC)*, pages 5213–5219. IEEE, 2016.

[198] Yuanqing Xia, Mengyin Fu, and Guo-Ping Liu. *Analysis and synthesis of networked control systems*, volume 409. Springer Science & Business Media, 2011.

[199] Lingyun Xiao and Feng Gao. Practical string stability of platoon of adaptive cruise control vehicles. *IEEE Transactions on intelligent transportation systems*, 12(4):1184–1194, 2011.

[200] Lingyun Xiao, Feng Gao, and Jiangfeng Wang. On scalability of platoon of automated vehicles for leader-predecessor information framework. In *2009 IEEE Intelligent Vehicles Symposium*, pages 1103–1108. IEEE, 2009.

[201] Gongjun Yan, Ding Wen, Stephan Olariu, and Michele C Weigle. Security challenges in vehicular cloud computing. *IEEE Transactions on Intelligent Transportation Systems*, 14(1):284–294, 2013.

[202] Xuanxia Yao, Xinlei Zhang, Huansheng Ning, and Pengjian Li. Using trust model to ensure reliable data acquisition in vanets. *Ad Hoc Networks*, 55:107–118, 2017.

[203] Sun Yi, Yi Sun, et al. *Time-delay systems: analysis and control using the Lambert W function*. World Scientific, 2010.

[204] Wente Zeng and Mo-Yuen Chow. A reputation-based secure distributed control methodology in d-ncs. *IEEE Transactions on Industrial Electronics*, 61(11):6294–6303, 2014.

[205] Hongwei Zhang, Frank L Lewis, and Abhijit Das. Optimal design for synchronization of cooperative systems: state feedback, observer and output feedback. *IEEE Transactions on Automatic Control*, 56(8):1948–1952, 2011.

[206] Linjun Zhang and Gábor Orosz. Nonlinear dynamics of connected vehicle systems with communication delays. In *2015 American Control Conference (ACC)*, pages 2759–2764. IEEE, 2015.

[207] Linjun Zhang and Gábor Orosz. Consensus and disturbance attenuation in multi-agent chains with nonlinear control and time delays. *International Journal of Robust and Nonlinear Control*, 2016.

[208] Yue Zhang, Christos G Cassandras, and Andreas A Malikopoulos. Optimal control of connected automated vehicles at urban traffic intersections: A feasibility enforcement analysis. In *American Control Conference (ACC), 2017*, pages 3548–3553. IEEE, 2017.

[209] Yue Zhang, Andreas A Malikopoulos, and Christos G Cassandras. Decentralized optimal control for connected automated vehicles at intersections including left and right turns. *arXiv preprint arXiv:1703.06956*, 2017.

[210] Jun Zheng and Abbas Jamalipour. *Wireless sensor networks: a networking perspective*. John Wiley & Sons, 2009.

[211] Y. Zheng, S. E. Li, K. Li, and L. Y. Wang. Stability margin improvement of vehicular platoon considering undirected topology and asymmetric control. *IEEE Transactions on Control Systems Technology*, 24(4):1253–1265, 2016.

[212] Yang Zheng, Shengbo Eben Li, Jianqiang Wang, Dongpu Cao, and Keqiang Li. Stability and Scalability of Homogeneous Vehicular Platoon: Study on the Influence of Information Flow Topologies. *IEEE Transactions on Intelligent Transportation Systems*, 17(1):14–26, 2016.

[213] Yang Zheng, Shengbo Eben Li, Keqiang Li, Francesco Borrelli, and J Karl Hedrick. Distributed model predictive control for heterogeneous vehicle platoons under unidirectional topologies. *arXiv preprint arXiv:1603.03225*, 2016.

[214] Yang Zheng, Shengbo Eben Li, Keqiang Li, Francesco Borrelli, and J Karl Hedrick. Distributed model predictive control for heterogeneous vehicle platoons under unidirectional topologies. *IEEE Transactions on Control Systems Technology*, 25(3):899–910, 2017.

[215] Yang Zheng, Shengbo Eben Li, Keqiang Li, and Wei Ren. Platooning of connected vehicles with undirected topologies: Robustness analysis and distributed h-infinity controller synthesis. *IEEE Transactions on Intelligent Transportation Systems*, 2017.

[216] Yang Zheng, Shengbo Eben Li, Keqiang Li, and Wei Ren. Platooning of connected vehicles with undirected topologies: Robustness analysis and distributed h-infinity controller synthesis. *IEEE Transactions on Intelligent Transportation Systems*, 19(5):1353–1364, 2018.

[217] Yang Zheng, Shengbo Eben Li, Jianqiang Wang, Dongpu Cao, and Keqiang Li. Stability and scalability of homogeneous vehicular platoon: Study on the influence of information flow topologies. *IEEE Transactions on Intelligent Transportation Systems*, 17(1):14–26, 2016.

[218] Yang Zheng, Shengbo Eben Li, Jianqiang Wang, Le Yi Wang, and Keqiang Li. Influence of information flow topology on closed-loop stability of vehicle platoon with rigid formation. In *2014 IEEE 17th International Conference on Intelligent Transportation Systems (ITSC)*, pages 2094–2100. IEEE, 2014.

[219] Jing Zhou and Huei Peng. Range policy of adaptive cruise control vehicles for improved flow stability and string stability. *IEEE Transactions on intelligent transportation systems*, 6(2):229–237, 2005.

[220] Yang Zhou, Soyoung Ahn, Madhav Chitturi, and David A Noyce. Rolling horizon stochastic optimal control strategy for acc and cacc under uncertainty. *Transportation Research Part C: Emerging Technologies*, 83:61–76, 2017.

[221] Feng Zhu and Satish V Ukkusuri. A linear programming formulation for autonomous intersection control within a dynamic traffic assignment and connected vehicle environment. *Transportation Research Part C: Emerging Technologies*, 55:363–378, 2015.

[222] Haojin Zhu, Rongxing Lu, Xuemin Shen, and Xiaodong Lin. Security in service-oriented vehicular networks. *Wireless Communications, IEEE*, 16(4):16–22, 2009.